REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE TECHNOLOGIE SAAD DAHLEB BLIDA 1

FACULTE DES SCIENCES

DEPARTEMENT D'INFORMATIQUE

Option : Sécurité des systèmes d'information

Thème :

Conception et automatisation d'un tableau de bord sécurité dans le cadre de la mise en œuvre de la PSI au sein de Sonelgaz

Sujet proposé par : Mme ABDOUS NADIA

Présenté par :

ADEL BAHIA

RAOUYA NIHEL

Encadré par :

Mme BOUMAHDI Fatima

Organisme d'accueil :

El Djazair Information Technology (ELIT) - SONELGAZ

Année universitaire: 2019 /2020

Dédicace

A nos chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de nos études,

A nos chères frères et sœurs pour leurs encouragements permanents, et leur soutien moral,

A toute notre famille pour leur soutien tout au long de notre parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fruit de votre soutien infaillible,

Merci d'être toujours là pour nous.

Remerciements

Nous remercions en premier lieu le bon Dieu le tout puissant qui nous à donner le courage, la volonté et la patience pour accomplir notre travail à temps.

Tout d'abord nous adressons un énorme remerciement et un profond respect à notre promotrice Madame ***BOUMAHDI FATIMA*** *et à notre chef d'option madame* ***BOUSTIA NARHIMENE,*** *signe de gratitude envers des personnes qui ont su être là, à nous apprendre, nous soutenir, nous corriger, nous guider et nous inspirer tout au long de notre parcours ; Nous les remercions pour l'aide et le temps précieux qu'ils ont bien voulu nous consacrer et sans qui ce travail n'aurait jamais vu le jour.*

Nous tenons aussi à remercier nos chers parents, et tous nos camarades avec lesquels on a partagé des moments mémorables.

On remercie aussi tous ceux qui ont contribué de près ou de loin pour accomplir notre travail de fin d'étude.

Finalement un grand merci à tous les enseignants du département d'informatique de BLIDA qui ont assuré notre formation durant nos cinq années d'étude.

Résumer

Pour programmer un tableau de bord sécurité, il ne convient pas de se lancer tête baissée dans l'écriture du code et générer, il faut d'abord avoir une idée primordiale sur la sécurité, se documenter et comprendre les notions essentielles afin de comprendre les étapes à suivre et réaliser enfin dans sa réalisation.

Pour créer notre tableau de bord nous avons tout d'abord pris connaissance des normes ISO/IEC 27002 et ISO/IEC 27004 afin de comprendre les domaines de la politique de sécurité de l'information de SONELGAZ, ensuite proposer des indicateurs de sécurité.

Après avoir proposé nos indicateurs nous avons établi une fiche technique pour chacun d'eux afin de les détaillées, connaitre leurs objectifs, proposer les formules de leur calcul, leur périodicité, et enfin le seuil de tolérance à ne pas dépasser, celui-ci est la référence de notre alerte de sécurité.

Nous avons aussi étudié les méthodes d'élaboration d'un bon tableau de bord sécurité et son fonctionnement afin d'organiser nos indicateurs dedans et enfin arriver à répondre aux besoins demander par notre entreprise de stage.

Mots clés : politique de sécurité de l'information, indicateur, tableau de bord.

Abstract

To program a security dashboard, it is not advisable to go headlong into writing the code and generating it, you must first have an essential idea about security, document yourself and understand the essential concepts in order to understand the steps to follow and finally achieve it. To create our dashboard, we first learned about ISO / IEC 27002 and ISO / IEC 27004 in order to understand the areas of SONELGAZ's information security policy, then propose security indicators. After having proposed our indicators we have established a technical sheet for each of them in order to detail them, know their objectives, propose the formulas for their calculation, their periodicity, and finally the tolerance threshold not to be exceeded, this is the reference of our security alert. We also studied the methods of developing a good safety dashboard and its functioning in order to organize our indicators in it and finally meet the needs requested by our internship company.

Keywords: information security policy, indicator, dashboard.

الملخص

لبرمجة لوحة معلومات أمنية، لا يُنصح بالمضي قدمًا في كتابة التعليمات البرمجية وإنشائها، يجب أن يكون لديك أولاً فكرة أساسية عن الأمان، وتوثيق نفسك وفهم المفاهيم الأساسية من أجل فهم الخطوات التي يجب اتباعها وأخيرا تحقيقها.
لإنشاء لوحة المعلومات الخاصة بنا، تعلمنا أولاً عن ISO / IEC 27002 و ISO / IEC 27004 من أجل فهم مجالات سياسة أمن المعلومات الخاصة بـ سونلغاز، ثم اقتراح مؤشرات الأمان.
بعد اقتراح مؤشراتنا، قمنا بإنشاء بطاقة تقنية لكل منها من أجل تفصيلها، ومعرفة أهدافها، واقتراح الصيغ لحسابها، وتواترها، وأخيرًا حد التسامح الذي لا يجب تجاوزه، وهذا هو إشارة تنبيه الأمان لدينا.
لقد درسنا أيضًا طرق تطوير لوحة معلومات أمان جيدة وعملها من أجل تنظيم مؤشراتنا فيها وتلبية الاحتياجات المطلوبة من قبل شركة التدريب لدينا.
الكلمات المفتاحية: سياسة أمن المعلومات، المؤشر، لوحة القيادة

TABLE DES MATIÈRES

Liste des figures

Liste des tableaux :

Liste des abréviations :

- **PSI :** Politique de Sécurité de l'Information.
- **SSI :** Sécurité des Systems d'Information.
- **ELIT :** El djazair Infomartion Technology.
- **SI :** Système d'Information.
- **SMSI :** Système de Management de la Sécurité Informatique**.**
- **DSI:** Direction des Systèmes D'information.
- **PDCA :** Plan Do Check Act.
- **ISO :** International Organization for Standarization.
- **IEC :** International Electrotechnical Commission.
- **API :** Application Programming Interface.
- **PHP :** Personal Home Page.
- **UML :** Unified Modeling Language.
- **SDK :** Software Development Kit.
- **JDK :** Java Development Kit.
- **XML :** Extensible Markup Language.
- **HTML :** Hypertext Markup Language.
- **IDE :** Integrated Development Environment.
- **SQL :** Structured Query Language.
- **SGBD :** Système de Gestion de Base de Données.
- **TCP :** Transmission Control Protocol.
- **IP :** Internet Protocol.
- **HTTP :** HyperText Transfer Protocol.
- **URL :** Uniform Resource Locator.
- **RAM :** Random Access Memory.
- **GPL :** Licence Publique Générale.
- **RH:** Ressource Humaine.

Introduction générale

Être en sécurité, c'est d'avoir la certitude de ne pas être atteint par une menace quelconque. Dans le monde informatique, cette définition aurait du mal à s'appliquer, tant que les menaces sont omniprésentes et multiformes.

Avec l'avènement du XXI^{e} siècle et le développement constant de la technologie, la sécurité est devenue un des enjeux majeurs de notre temps.

Avec tous les outils de communication que nous utilisons aujourd'hui (Smartphone, ordinateur portable, tablette, connexion wifi, connexion Bluetooth, connexion internet, etc…) **[1]**, les entreprises évoluent dans un environnement de plus en plus incertain. Confrontées à une concurrence rude, une obligation de performance et des menaces extravagantes, la mise en place d'un système de sécurité s'avère être une condition capitale pour survivre et se développer tout en étant serin **[2].**

Pour mieux contribuer à la sécurité des entreprises, les experts de l'organisation internationale de normalisation (ISO) ont élaboré des normes internationales d'application volontaire, fondées sur le consensus, pertinentes pour le marché, soutenant l'innovation et apportant des solutions aux enjeux mondiaux.

A chaque norme un domaine précis, dont la norme ISO/IEC 27002 intitulé code de bonnes pratiques, qui a contribuée à respecter les démarches de sécurité et à élaborer la politique de sécurité de l'information (PSI) propre et unique à l'organisation SONELGAZ en particulier par les ingénieurs de sécurité de la filiale ELIT.

Cette PSI définit les objectifs et les mécanismes d'organisation de sécurité de l'information au sein de notre organisation, elle se compose en elle-même de plusieurs démarches et domaines, plus précisément de quatorze domaines qui sont eux même les chapitres de la norme ISO/CEI 27002, ils nous ont était transmis en documents confidentiels par ELIT. Après une étude détaillée et approfondie de ces domaines nous allons définir dans les chapitres qui suivent les différents indicateurs de sécurité adaptés à chaque domaine de la PSI.

Face à la complexité des systèmes à risques, l'évaluation des performances de sécurité avec des outils simplistes peut s'avérer préjudiciable aux décideurs et ingénieurs qui ne seraient pas conscients de leurs travers.

Tenant compte de leurs larges divergences qui demeurent sur leurs rôles, des apports et modalités d'utilisation qu'ils apportent au quotidien, le recours aux indicateurs de sécurité dans les systèmes d'information devient une nécessité de notre temps.

De manière très générale, l'indicateur peut être définit comme un élément ou une information qui fournit des indications. En sécurité informatique ces indicateurs sont destinés aux responsables sécurité des systèmes d'information, directeurs sécurité des systèmes d'information, manager de risques … etc. Ces indicateurs ont pour vocation d'alimenter des tableaux de bords destinés à plusieurs cibles, directions générales ou pilotes opérationnels, ce qui définit qu'ils sont partagés en deux types stratégiques et opérationnels.

Encore une fois l'ISO est là pour nous aider à proposer des indicateurs pertinents est spécifiques à chaque domaine le PSI grâce à la norme ISO/IEC 27004.

Le tableau de bord s'avère être un outil d'aide à la décision, très largement utilisé dans le domaine de la gestion des grandes entreprises comme SONELGAZ. En récoltant les informations nécessaires à l'établissement des indicateurs de sécurité, le tableau de bord se transforme en une compilation d'un nombre important d'informations numériques pour devenir une véritable banque de données. Ces données sont essentielles pour faire des prévisions de risques et contrôler la sécurité des multiples filiales de SONELGAZ.

Face aux différents conflits de sécurité, la socité SONELGAZ a rencontré la problématique suivante : comment implémenter une solution simple et compréhensive pour avoir un meilleur suivit de la PSI aux niveaux sociétés du Groupe SONELGAZ ?.

Afin de trouver une solution, l'objectif de notre travail est d'établir un tableau de bord avec des indicateurs pertinents, cet outil sera indispensable pour permettre aux différentes instances (ELIT, RSI, COSIG) d'avoir une vue réelle sur l'avancement du projet et la mise en place des mesures de sécurité.

-Structure du mémoire:

Ce mémoire s'articule en plusieurs parties. Tout d'abord, une première partie, permettant de mieux définir le contexte de notre travail, elle est consacré aux principales definitions et objectifs de la politique de sécurité de l'information, de la norme qu'ELIT a suivi pour son élaboration, mais aussi des indicateurs.

En seconde partie, passant aux tableaux de bord, le tableau de bord sécurité est un outil qui va donner une vision de synthèse du niveau de risque. Pour sa conception nous devons connaitre les règles de bases et la méthode adaptée, afin de proposer le tableau ideal.

La troisième partie, est consacrée à notre proposition , ainsi nous parlerons de la norme ISO/IEC 27004 dont la méthode inclue nous a aidé à proposé nos indicateurs, définir leurs avantages et leurs différents usages, nous afficherons aussi une fiche technique pour chaque indicateur afin de mieux le cerner et le comprendre.

Donc effectivement la quatrième partiee sera consacrée à la conception de notre solution et la cinquième à la réalisation et l'implémentation de cette solution.

Chapter 1 : Ètat de l’art

I.1) Introduction :

Les risques en matière de sécurité n'ont cessé d'augmenter ces dernières années, il est important pour les entreprises de, mettre en place une politique de sécurité de l'information qui permettra la mise en place de mécanismes servant à réduire les risques liés à la gestion de l'information produite ou reçue. Cette information consiste notamment en des renseignements personnels, professionnels ou des informations stratégiques ou opérationnelles de l'administration qui peuvent être représenter avec des indicateurs de sécurité.

I.2) Politique de sécurité de l'information :

Est un ensemble formalisé des éléments stratégiques, des directives, procédures, codes de conduite, règles organisationnelles et techniques, ayant pour objectif la protection du (des) système(s) d'information de l'organisme. **[3]**

I.3) Nécessité de la PSI :

Face aux différente menaces la nécessité de la PSI se présente comme suit :

- La PSI traduit la reconnaissance formelle de l'importance accordée par la direction générale de l'organisme à la sécurité de son ou ses systèmes d'information.
- La sécurité est donc devenue l'une des dimensions essentielles de la stratégie de l'organisme et elle doit être prise en compte dès la conception d'un système d'information afin d'assurer la protection des biens et des personnes et du patrimoine de l'organisme.
- La sécurité des systèmes d'information vise en particulier à protéger les composantes du patrimoine matériel, immatériel et intellectuel ainsi que les informations relatives aux personnes (physiques et morales).
- La PSI définit la politique de sécurité d'une entité spécifique qui peut être un système technologique, une fonction automatisée ou une application mais aussi un organisme entier comme une entreprise ou un département ministériel. Une entreprise repose sur son personnel, sa culture, ses informations et ses processus de gestion (traitement, stockage ou/et transfert) des informations. Ce sont ces processus d'entreprise qui font toute la différence entre deux "organisations" au but similaire, dans le même secteur économique.
- La PSSI constitue un cadre de référence et de cohérence :

  - pour l'intégration de la sécurité lors de la conception d'un système d'information.

  - pour l'ensemble des activités et des acteurs de l'organisme par rapport auxquels toute évolution du système d'information devra être justifiée.

- pour aider les personnes chargées d'élaborer et de mettre en œuvre des mesures, des consignes et des procédures cohérentes en vue d'assurer la sécurité des systèmes d'information. **[4]**

I.4) Les objectifs visés par la PSI :

Une politique de sécurité vise les objectifs suivants :

- D'assurer que les utilisateurs observent les bonnes pratiques et les règles quant à l'utilisation des technologies de l'information;
- D'assurer que les normes en matière de sécurité informatique soient dûment mises en application
- De réviser périodiquement les résultats des vérifications et contrôles, notamment pour y relever les anomalies et autres incidents
- De recommander les actions à prendre pour corriger les situations anormales ou dangereuses, notamment, les processus opérationnels et les grandes stratégies en matière informatique et les achats d'équipement.
- D'informer le comité de Direction générale des travaux, activités et incidents en matière de sécurité informatique.
- D'assurer que les éléments opérationnels qui requièrent une approbation des différentes directions soient respectés. **[5]**

I.5) Lignes directrices pour la sécurité :

La PSI vise à assurer la protection des droits de l'entreprise et le respect par l'Institut de la réglementation en matière de confidentialité, de protection des personnes et de propriété intellectuelle et industrielle. Elle offre:

- Protection de l'infrastructure des systèmes d'information.
- Protection des données.
- Protection juridique.

Et des Critères de sécurité :

La teneur des critères de sécurité à envisager peut-être décrite de la façon suivante :

a) Disponibilité : désigne le fait que les données considérées sont accessibles au moment voulu par les utilisateurs autorisés.
b) Intégrité : les données ne sont pas corrompues ni modifiées de façon non autorisée.
c) Authenticité : les données disponibles sont bien celles que l'établissement souhaite divulguer, et seulement elles.

d) Confidentialité : les données ne sont disponibles que pour ceux auxquels elles sont destinées.

e) Non répudiation : les données publiées de façon authentique sont certifiées, et leur auteur ne peut pas nier les avoir publiées, il en assume la responsabilité. **[6]**

I.6) Domaines d'application de la PSI :

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

La PSSI :

- S'applique à un système existant ou à développer.
- Concerne toute personne ayant accès au système d'information de l'entreprise qu'il soit interne ou externe à l'organisme (sous-traitant, stagiaire, prestataire).
- Concerne l'ensemble des aspects du système d'information (l'organisation, l'environnement physique, le développement, l'exploitation, la maintenance…).
- Concerne l'ensemble du cycle de vie du système d'information et de l'information.

Donc en général elle couvre l'ensemble des systèmes d'information de l'administration, de l'organisme ou de l'entreprise. **[7]**

I.7) Démarche de réalisation et de mise en œuvre d'une PSI :

I.7.1) Présentation de la démarche :

La démarche, qui est menée sous la forme d'un "projet PSSI", se base sur le référentiel de l'organisme et une analyse des risques SSI.
Le référentiel SSI de l'organisme (schéma directeur, meilleures pratiques, directives internes…) et une analyse des risques préalables fournissent en effet les éléments permettant d'effectuer et de justifier les choix, de légitimer l'action et de garantir la cohérence avec le contexte particulier de l'organisme.
L'objectif de la méthode consiste à construire un document de politique comprenant des éléments stratégiques et des règles de sécurité pour un organisme ou un système d'information.
La validation successive des différentes phases vise à faciliter l'implication de la Direction générale et l'adhésion de tous les intervenants. **[8]**

La figure suivante présente la démarche en 4 phases :

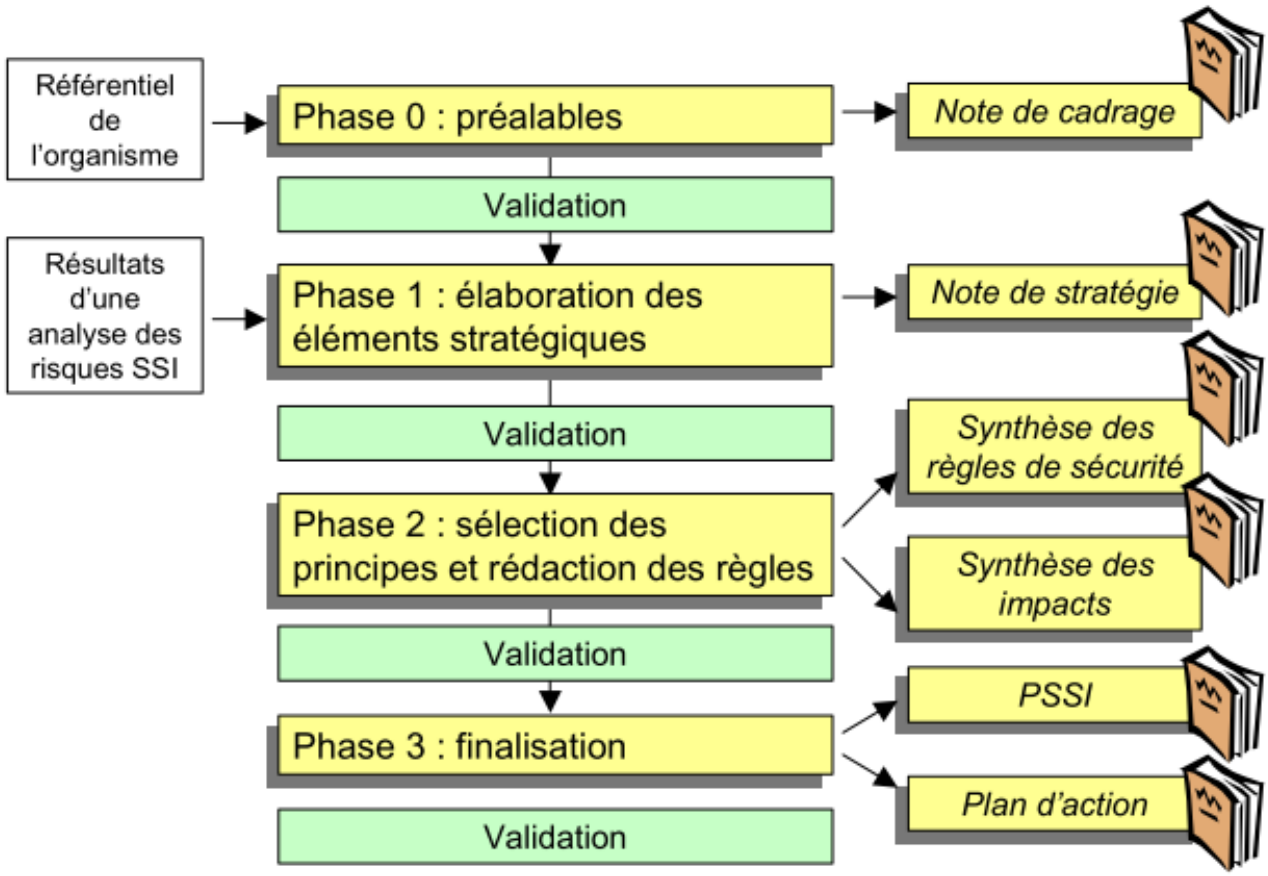


Figure I.7.1: Présentation générale de la démarche [8].

I.7.2) Démarche d'élaboration d'une PSI [9]:

Le déroulement de la méthode exige principalement :

- Une implication forte de l'encadrement au plus haut niveau.
- De disposer de moyens humains significatifs, non seulement pour le chef de projet responsable du projet mais aussi pour l'ensemble des acteurs impliqués (techniques, fonctionnels et décisionnels).
- Une implication active et une motivation réelle de l'ensemble des acteurs, notamment celle des responsables techniques et fonctionnels ;
- La prise en compte de moyens financiers et humains pour la mise en œuvre future du plan d'action produit par l'étude.
- La prise en compte des pratiques et usages du système d'information par les différents profils d'acteur pour éviter de révolutionner les méthodes de travail qui ont, dans la plupart des cas, fait leur preuve.

Il est précisé en outre que ce type de démarche n'a de sens que si :

- Elle est menée de façon consensuelle avec des points de validation successifs réguliers.
- Les éléments étudiés le sont dans leur globalité, c'est à dire que l'étude doit s'intéresser, pour un système donné, à l'ensemble des risques et à l'ensemble des moyens de sécurité à mettre en œuvre tous les aspects des systèmes et de leur environnement tant physique qu'organisationnel.
- Elle est réalisée par un tiers (prestation d'assistance) qui, de par sa position de neutralité pourra faire émerger les éléments nécessaires à l'élaboration d'une PSSI en franchissant plus facilement les barrières interpersonnelles.

I.7.3) Aperçu des différentes phases de la PSI :

I.7.3.1) **Phase 0 : préalables**

Cette phase préliminaire doit permettre la présentation du projet au niveau de la Direction générale et de faire valider ainsi ses objectifs et les moyens qu'il convient d'y consacrer. **[10]**

<table>
<tr><td colspan="2">Objectifs de la phase
Définir les objectifs et moyens à mettre en œuvre pour l'élaboration de la PSSI et constituer le référentiel documentaire.</td></tr>
<tr><td colspan="2">Acteurs de la phase
- Le responsable sécurité ou l'initiateur du projet PSSI</td></tr>
<tr><td>Éléments en entrée
- Référentiel de l'organisme</td><td>Éléments en sortie
- Note de cadrage
- Référentiel documentaire</td></tr>
<tr><td colspan="2">Tâches
1. Décrire l'organisation du projet
2. Constitution du référentiel documentaire</td></tr>
<tr><td colspan="2">Observations</td></tr>
<tr><td colspan="2">Cette phase doit permettre à la Direction générale de prendre la décision de lancement de l'opération sur la base d'un cadre formalisé d'intervention définissant les objectifs et moyens à mettre en œuvre.</td></tr>
<tr><td colspan="2">Validation</td></tr>
<tr><td>Documents</td><td>Validateur</td></tr>
<tr><td>Note de cadrage</td><td>Hiérarchie au plus haut niveau, par défaut la Direction Générale</td></tr>
</table>

Figure I.7.2 : Fiche de synthèse pour la phase 0. [10]

I.7.3.2) **Phase 1 : élaboration des éléments stratégiques [10] :**

Objectifs de la phase Cette phase, dont les résultats et conclusions doivent impérativement être validés par la Direction Générale, consiste à déterminer les axes stratégiques et les premières grandes orientations à partir desquelles sera déclinée la PSSI. Pour cela, elle doit obligatoirement identifier et prendre en compte le périmètre d'étude, le contexte, les enjeux et orientations stratégiques, le référentiel réglementaire, l'échelle de besoins, les besoins de sécurité des biens à protéger et les origines des menaces afin d'aboutir à une note de stratégie validée par la Direction fixant les grandes orientations de la SSI.
Acteurs de la phase - Chef de projet - Représentants de la maîtrise d'ouvrage - Direction Générale - Responsable juridique

Éléments en entrée	**Éléments en sortie**
- Référentiel documentaire	- Note de stratégie de sécurité

Tâches 1. Délimitation du périmètre 2. Identification des enjeux et orientations stratégiques 3. Recensement des lois et règlements applicables 4. Définition d'une échelle de besoins en termes de disponibilité, intégrité, confidentialité et éventuellement d'autres critères de sécurité 5. Expression des besoins de sécurité des biens à protéger 6. Identification des origines des menaces pesant sur l'organisme ou le système étudié (et éventuellement des principaux risques et objectifs de sécurité)
Observations
Il convient d'insister sur l'importance capitale de cette phase et sur la nécessité d'une implication forte de la Direction Générale tant lors de l'identification des besoins et menaces que lors de la validation de la cible et des principaux objectifs à atteindre.
Validation

Document	**Validateur**
Note de stratégie de sécurité	Comité de pilotage puis Direction générale

Figure I.7.3 : Fiche de synthèse pour la phase 1. [10]

I.7.3.3) **Phase 2 : sélection des principes et rédaction des règles [10]:**

<table>
<tr><td colspan="2">Objectifs de la phase
Le travail de cette phase consiste à sélectionner, concevoir, préparer, documenter et valider la déclinaison des principes généraux d'une PSSI et des choix stratégiques de l'organisme. Ce travail se traduit en l'élaboration d'un corpus de règles directement applicables.</td></tr>
<tr><td colspan="2">Acteurs de la phase
- Direction générale
- Comité de pilotage
- Groupe d'experts</td></tr>
<tr><td>Éléments en entrée
- Note de cadrage
- Note de stratégie de sécurité</td><td>Éléments en sortie
- Note de synthèse justificative des choix de règles
- Note de synthèse des impacts organisationnel et financier</td></tr>
<tr><td colspan="2">Tâches
1. Sélection des principes
2. Construction des règles
3. Synthèse et validation</td></tr>
<tr><td colspan="2">Observations</td></tr>
<tr><td colspan="2">Les points essentiels à prendre en compte sont la cohérence des règles, leur applicabilité et enfin l'auditabilité de l'ensemble.</td></tr>
<tr><td colspan="2">Validation</td></tr>
<tr><td>Documents</td><td>Validateur</td></tr>
<tr><td>Note de synthèse justificative des choix de règles
Note de synthèse des impacts organisationnel et financier</td><td>Comité de pilotage puis Direction générale</td></tr>
</table>

Figure I.7.4 : Fiche de synthèse pour la phase 2 [10].

I.7.3.4) **Phase 3 : finalisation [10] :**

Objectifs de la phase La finalité de cette phase est de conduire une étape ultime de validation de la PSSI et du plan d'action associé par la direction générale	
Acteurs de la phase - Comité de pilotage - Groupe d'experts	
Éléments en entrée - Les règles retenues validées	**Éléments en sortie** - La PSSI validée - Plan d'application de la PSSI proposant en particulier un plan d'action selon les priorités définies
Tâches 1. Finalisation et validation de la PSSI 2. Élaboration et validation du plan d'action	
Observations	
Une fois la PSSI revue et validée par le comité de pilotage, un document de synthèse devra être élaboré pour soutenir la présentation de la PSSI à la hiérarchie en vue de sa validation. L'implication des différents acteurs, notamment des futurs responsables de la mise en œuvre de la PSSI, est fondamentale pour disposer par la suite des ressources humaines et financières adéquates et prévoir les délais. C'est à ce niveau que se mesure l'importance de l'implication des experts lors de la déclinaison des principes et objectifs généraux dans les différents domaines. Cela montre également l'importance de l'applicabilité comme critère essentiel lors du choix et de la formalisation des règles. La validation du plan d'action doit passer par une étape de simplification de la PSSI pour transmettre les messages forts à la Direction Générale.	
Validation	
Documents	**Validateur**
PSSI Plan d'action	Comité de Pilotage puis Direction générale

Figure I.7.5 : Fiche de synthèse pour la phase 3 [10].

I.7.4) Principaux résultats de la méthode [11] :

L'élaboration de la PSI doit permettre de :

1) Disposer d'un cadre de référence et de cohérence pour l'ensemble des activités et des acteurs de l'organisme.

Ce cadre de sécurité doit notamment permettre la mise en évidence des objectifs, obligations et engagements de l'organisme vis-à-vis de ses partenaires, clients et sous-traitants, ainsi que les principes de sécurité régissant la protection de son propre patrimoine.

Ce cadre fondamental et fédérateur doit exprimer les responsabilités de l'ensemble des acteurs, ainsi que les principes et règles de sécurité minimaux à respecter pour l'ensemble des activités et des systèmes.
Il doit offrir les directives nécessaires, notamment pour tout choix technique mais aussi organisationnel ou contractuel, en matière de sécurité, et permet d'assurer la cohérence et la pérennité des actions de sécurité.

Constituer un document général diffusable
La Politique de Sécurité des Systèmes d'Information doit être connue de l'ensemble des acteurs internes, ainsi que, le cas échéant, de l'ensemble des personnes accédant au SI de l'organisme (prestataires, sous-traitants, stagiaires).
Le document doit être largement diffusé, éventuellement sous une forme simplifiée et didactique (le langage utilisé doit être approprié aux destinataires), à l'ensemble du personnel. Cette diffusion sera, le cas échéant, accompagnée d'une sensibilisation de l'ensemble du personnel portant sur le rappel des principes, de l'organisation et des règles de sécurité. **[11]**

I.8) Norme contribuant à la définition d'une politique de sécurité :

I.8.1) Norme ISO/IEC 27002:

- La norme ISO/IEC 27002, sous l'intitulé « Technologies de l'information - Techniques de sécurité -Code de bonne pratique pour le management de la sécurité de l'information » a été publiée en 2005 et révisée en 2013. Elle offre des lignes directrices en matière d'instructions organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité, en prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation. La norme ISO 27002 :2013 est élaborée à l'intention des organisations désireuses de sélectionner les mesures de sécurité nécessaires dans le cadre du processus de mise en œuvre d'un Système de Management de la Sécurité de l'Information (SMSI) en se basant sur la norme ISO/CEI 27001 (ISO/CEI 27002, 2013) **[12]**.

I.8.2) Domaine d'application:

L'ISO 27002 a pour objectif d'aider à l'évaluation et au traitement des risques de sécurité des informations liés à la confidentialité, l'intégrité et aux aspects de la disponibilité.

Elle fait application du modèle de gestion de la qualité PDCA (Plan Do Check Act) **[13]**.

I.8.3) Structure de la Norme ISO 27002 :

La Norme ISO 27002 inclut 15 chapitres.

Les 4 premiers sont des chapitres d'introduction, et les 11 suivants sont déstinés aux aspects stratégiques et opérationnels du management de la sécurité et représentent ses objectifs principaux à atteindre **[14]** :

- Chapitre 5. Politique de sécurité.
- Chapitre 6. Organisation de la sécurité de l'information.
- Chapitre 7. Gestion des biens (actifs/assets) – des biens physiques, des informations, des logiciels, des services de la documentation.
- Chapitre 8. Sécurité des ressources humaines.
- Chapitre 9. Sécurité physique et de l'environnement.
- Chapitre 10. Gestion des communications et des opérations.
- Chapitre 11. Contrôle d'accès.
- Chapitre 12. Acquisition, développement et maintenance des systèmes d'informations.
- Chapitre 13. Gestion des incidents à la sécurité de l'information.
- Chapitre 14. Gestion du plan de continuité de l'activité.
- Chapitre 15. Conformité avec les réglementations, les lois et la politique de sécurité.

I.9) Les Indicateurs :

Un indicateur est un élément ou un ensemble d'éléments d'information significative, un indice représentatif, une statistique ciblée et contextualisée, selon une préoccupation de mesure, résultant de la collecte de données sur état, sur la manifestation observable d'un phénomène ou sur un élément lié au fonctionnement d'une organisation. **[15]**

I.10) Objectifs des indicateurs :

Les objectifs des indicateurs, regroupés sous forme de « tableau de bord », sont :

▪ Suivre la qualité des services de sécurité,
▪ Suivre la qualité de la politique de sécurité établie,
▪ Remonter les alertes afin de prévenir les dysfonctionnements,
▪ Fournir un outil synthétique d'aide au système d'assurance et de gestion de la sécurité. **[16]**

I.11) Typologie des indicateurs [17] :

Plusieurs critères peuvent être utilisés pour classer les indicateurs :

- Indicateur de résultat ou de progression : information sur le résultat d'une action finie ou sur une action en cours.
- Indicateur financier ou non financier.

- Indicateur global ou ponctuel : un indicateur peut être synthétique, calculé à partir de plusieurs informations pour donner une image à plusieurs dimensions ou au contraire très ciblé sur un seul paramètre très précis.
- Indicateur de pilotage : un indicateur peut être demandé par un niveau hiérarchique en vue de contrôler des engagements, mais il peut aussi aider le responsable à orienter son action ; c'est plutôt l'orientation actuelle donnée aux indicateurs. **[17]**

I.12) Les caractéristiques d'un bon indicateur [18]:

Les caractéristiques générales que l'on recherche pour un indicateur sont les mêmes que pour tout instrument de mesure et de reportage. De façon générale, nous cherchons à respecter plusieurs critères, que nous regroupons en quatre volets, pour nous assurer de la valeur optimale et de sa maturité

- ✓ Sa pertinence,
- ✓ La qualité et la précision de sa mesure,
- ✓ Sa faisabilité
- ✓ Sa préoccupation d'interprétation d'utilisation.

La méthode de réalisation des tableaux de bord aborde d'ailleurs des considérations et propose des outils pour s'assurer de répondre à chacun de ces critères.

La pertinence de l'indicateur doit correspondre à une préoccupation, à un objectif ou à une attente. Il doit répondre au besoin de mesure, avoir une signification dans le contexte d'étude ou de gestion, il doit vouloir dire quelque chose pour ses utilisateurs et être utilisé dans ce contexte. On doit tendre à donner à l'indicateur la valeur ajoutée maximale par sa mise en perspective par rapport à des balises pertinentes (objectifs, marges acceptables, valeurs comparatives, etc.).

L'indicateur doit posséder certaines caractéristiques intrinsèques :

- ➢ La clarté et la précision de sa formulation,
- ➢ Une qualité théorique (une formulation et une logique d'articulation correspondant aux définitions reconnues du domaine),
- ➢ Une bonne formulation, précise, avec des paramètres bien établis (ventilations, périodicité, comparaisons, forme de présentation)
- ➢ Bien documenté. En outre, il doit être assez sensible pour faire ressortir toute variation significative de l'objet de mesure et assez homogène dans le temps et dans l'espace pour permettre :
  - ▪ <u>La comparabilité :</u> Les paramètres de comparaison doivent être assez stables pour permettre la consistance des comparaisons dans le temps (par exemple, l'amélioration du taux de réussite ne veut pas dire grand-chose si on a réduit la difficulté des examens). On parle aussi de fidélité.
  - ▪ <u>L'adaptabilité :</u> Les paramètres doivent être suffisamment souples pour permettre l'adaptation de l'indicateur aux particularités sectorielles, tout en gardant sa valeur

intrinsèque. La documentation de l'indicateur doit clairement mentionner ces particularités pour en permettre l'interprétation contextuelle correspondante.

- La spécificité et la focalisation : Les indicateurs doivent être structurés de façon à bien cerner l'objet de la mesure, à bien décoder la situation dans le bon registre, à l'utiliser dans le bon référentiel, dans le bon contexte décisionnel. On vise, entre autres, à éviter la surinformation qui finit par ne plus rien signifier. **[18]**

I.13) Les indicateurs opérationnels et indicateurs stratégiques :

L'indicateur peut correspondre et servir à un ou à plusieurs paliers hiérarchiques de l'organisation. On pourrait ainsi avoir des indicateurs opérationnels, des indicateurs stratégiques, des indicateurs professionnels (ou cliniques, dans le domaine de la santé) liés aux interventions, etc. On pourrait aussi avoir divers panoramas d'un même indicateur ventilé selon le palier visé. De fait, il est parfois difficile de distinguer clairement les indicateurs par palier hiérarchique en utilisant ces qualificatifs habituels (opérationnels et stratégiques).

1) Les indicateurs opérationnels : sont liés au fonctionnement même de l'organisation : interventions et dispensation de service aux clients, processus d'affaire, utilisation des ressources, résultat de production, etc. Ils ont en général une périodicité assez courte et doivent être suivis régulièrement afin d'apporter les correctifs appropriés sur le terrain. Ils s'arriment en général assez bien aux systèmes d'information de gestion.

2) Les indicateurs stratégiques : pour leur part, sont liés à la mission et aux objectifs de l'organisation; ils sont plus complexes à traiter. D'abord, ils nécessitent souvent à la fois des mesures internes sur les capacités de l'organisation et ses choix de missions et des mesures externes sur les besoins et les exigences de l'environnement, souvent difficiles à mesurer. Certains des indicateurs de niveau ou de type stratégique reprennent et synthétisent les indicateurs opérationnels jugés névralgiques, de façon synoptique et sur un horizon temporel plus large. Ces indicateurs correspondent aux attentes fondamentales, aux axes de réussites, aux facteurs critiques de succès, en général en conformité avec les divers plans d'intervention établis. Ils sont orientés à la fois sur la pertinence et l'efficacité externe (résultats pro- duits, coûts et effets des activités ou des programmes sur la clientèle) et sur l'efficacité interne et l'efficience (résultats atteints, ressources et coûts). Les principaux indicateurs de ce niveau sont souvent constitués à partir de résultats synoptiques du type de ceux publiés dans les bilans et les rapports annuels traditionnels. **[19]**

I.14) Conclusion :

En conclusion nous avons abordé dans ce chapitre l'importance majeure d'élaborer une PSI dans les entreprises, ses différent domaines et démarches ainsi que la notions des indicateurs et leurs types que nous allons organiser dans un tableau de bord

Chapter 2 :
Tableaux de bord

II.1) Introduction :

Face à l'évolution constante des besoins fonctionnels et des outils informatiques, il est de devenue nécessaire pour les entreprises de maîtriser les coûts engagés dans les investissements informatiques, d'en mesurer toutes les valeurs ajoutées et de s'assurer de leur efficacité. Ceci répond à un objectif d'amélioration permanente de l'organisation, tant au niveau opérationnel que stratégique.
Dans ce contexte l'établissement d'un tableau de bord s'avère être l'outil idéal pour un meilleur contrôle.

II.2) Définition tableau de bord SSI :

Un tableau de bord est un outil d'aide à la décision et à la prévision, il est un ensemble d'indicateurs conçu pour permettre aux gestionnaire de prendre connaissance de l'état et l'évolution des systèmes qu'ils pilotent et d'identifier les tendances qui les influenceront sur un horizon cohérent avec la nature de leurs fonctions. **[20]**

D'une autre manière est un ensemble cohérent d'indicateurs mis en forme et agencés de manière à présenter une image synthétique de la situation de la sécurité du système d'information considéré. **[21]**

II.3)Le tableau de bord, une interface intégratrice :

En soi, un tableau de bord n'est pas et ne remplace pas le système d'information de gestion.

C'est une interface intégratrice entre un système de gestion, un système de mesure, un système d'information et des utilisateurs ; il permet de sélectionner, consolider, agencer et présenter, de façon rapide et sommaire, l'information essentielle à la gestion, par un nombre restreint d'indicateurs significatifs se rapportant aux clients, aux ressources, aux activités, aux résultats et à l'environnement de l'organisation.

C'est une interface, car il représente une structure intermédiaire d'accès à l'information par navigation et forage, de filtrage, de réorganisation et de présentation de cette information pertinente à la gestion. Pour cela, il requiert un bon système d'information qui l'alimente en données. Remarquons qu'il ne peut en aucun cas remplacer un reportage de suivi opérationnel régulier et détaillé produit par un système d'information de gestion. **[22]**

II.4) Objectif et élaboration d'un tableau de bord SSI :

Un tableau de bord parfaitement adapté à chaque type de fonction de la "voie fonctionnelle SSI" est un atout pour améliorer la qualité des services de sécurité et maîtriser le niveau de sécurité global de sécurité des systèmes d'information.

Les objectifs justifiant la mise en place d'un tableau de bord de la DSI sont multiples, tout comme les destinataires de l'outil qui sera élaboré (Direction Générale, Direction Administrative et Financière, Direction des Systèmes d'Information de groupe...). Cette diversité d'utilisateurs potentiels entraîne inévitablement une multiplicité des besoins, exprimés ou non. La première étape est donc de déterminer, et de valider, les objectifs assignés au projet. **[23]**

Le tableau de bord constitue en effet un outil de synthèse et de visualisation indispensable pour suivre toutes les actions liées à la SSI. Il contribue à contrôler que la stratégie définie dans la politique de sécurité est mise en œuvre par les niveaux de pilotage et opérationnel, et à la remontée d'informations pertinentes jusqu'aux décideurs.

Pour le niveau stratégique, la mise en place d'un tableau de bord permet :

- ✓ De suivre l'application de la politique de sécurité,
- ✓ D'établir des comparaisons avec d'autres organismes,
- ✓ De préparer les choix de mise en place des ressources (définition de priorités, réévaluation de la menace et du risque).

Pour le niveau de pilotage, la mise en place d'un tableau de bord permet :

- ✓ De contrôler la réalisation des objectifs par le niveau opérationnel,
- ✓ D'améliorer la qualité de service.

Pour le niveau opérationnel, la mise en place d'un tableau de bord permet :

- ✓ De préciser les besoins opérationnels à mettre en œuvre,
- ✓ De mesurer la production et les efforts entrepris pour atteindre les objectifs visés en matière de production,
- ✓ De motiver et dynamiser les équipes. **[24]**

II.5) La conception du tableau de bord de la DSI :

La validation des objectifs permet au projet de passer à la définition des orientations du futur tableau de bord. Cette phase a pour finalité de déterminer le choix des indicateurs à intégrer dans l'outil. Dans la méthodologie à adopter, trois grandes phases sont primordiales, sans pour autant être exhaustives et suffisantes :

- Le choix des dimensions fonctionnelles à suivre, mesurer et piloter.

- Le choix des indicateurs potentiels à retenir, qui doivent être en phase avec les dimensions fonctionnelles définies précédemment.
- Le choix d'un outil technique en parfaite adéquation avec les besoins et les objectifs.

La dimension financière :

La dimension financière est un axe de mesure principal de l'efficacité de la DSI. Dans un contexte d'intégration poussée des outils informatiques dans toutes les fonctions de l'organisation, la Direction Générale est particulièrement sensible aux indicateurs liés à l'impact financier. L'analyse de la dimension financière a plusieurs finalités. Elle permet notamment d'effectuer des observations par rapport au reste de l'entreprise, et de mesurer l'efficacité des investissements informatiques proprement dits.

Les indicateurs possibles pour cet axe d'analyse sont : la part de budget SI rapportée au volume globale des investissements, le retour sur investissements des projets SI, la répartition du budget SI …etc.

La dimension « Relation client fournisseur » :

La relation « client fournisseur » mesure la qualité des prestations de l'ensemble de l'équipe informatique envers le reste de l'organisation. Elle mesure à la fois l'efficacité des hommes, des outils informatiques mis à la disposition des collaborateurs ainsi que leur adéquation aux besoins exprimés. La mesure de la relation client fournisseur est basée sur un ensemble d'engagements de la DSI (le « contrat de service ») pour offrir une meilleure qualité de service au moindre coût. Pour atteindre cet objectif, il est indispensable de formaliser le lien entre la DSI et ses différents clients internes ou externes. La création de l'outil de suivi et de pilotage permet de faire vivre ce lien.

La mesure de la performance des équipes de la DSI dans ce cadre peut s'effectuer grâce aux indicateurs tels que le niveau de service atteint par les activités de support, le niveau de service ou de disponibilité des applications, le respect des engagements pris dans le cadre du « Contrat de service », la qualité de la relation métier-DSI, …etc.

La dimension organisationnelle :

La mesure de l'efficacité organisationnelle vise à déterminer la qualité des processus au sein desquels intervient la DSI. Il s'agit des processus propres à la DSI comme ceux liés aux différents métiers de l'organisation au sein desquels interviennent les équipes informations. Cette dimension va donc bien au-delà des aspects liés aux activités de supports. Elle mesure également l'implication de la DSI dans les différents projets transversaux de l'entreprise et aborde les notions de normes et standards.

Quelques indicateurs performants pour suivre et piloter l'efficacité organisationnelle sont : l'efficacité des processus (métier, SI), l'efficacité du SI, le respect des normes et standards, l'efficacité dans le management des projets, le taux de satisfaction des relations avec les prestataires externes …etc.

La dimension « perspectives d'évolution » du SI :

La performance de l'ensemble du système d'information se mesure également à sa pérennité. Pour chaque brique du système, la direction des systèmes d'information et la direction générale se doivent de connaître les perspectives d'évolution, tant techniques que fonctionnelles des outils dont l'organisation dispose. Plusieurs axes d'analyse, donc de mesure, sont à prendre compte :

- La pérennité des différentes technologies utilisées (par rapport aux tendances informatiques essentielles).
- L'existence de connaissances et compétences internes ou externes pour gérer et faire évoluer les outils actuels.
- La capacité des outils à évoluer, à intégrer et à s'intégrer à d'autres standards notamment dans un contexte où se succèdent les rapprochements entre firmes. La compatibilité des différents systèmes d'information constitue un facteur clé de réussite de ces opérations de fusions/acquisitions. L'existence d'un tableau de bord fiable et complet constitue ainsi une base de travail essentielle.
- Les indicateurs basiques pour mesurer l'évolutivité du système d'information sont : le taux de maintenabilité ou de modularité du système, l'adaptabilité et la flexibilité, la modernité…etc. **[25]**

II.6) Les règles de base de la construction du tableau de bord de la DSI :

Lors du lancement du projet de conception d'un tableau de bord de la DSI, quelques règles simples de gestion de projet sont indispensables :

- La prise en compte des avis des utilisateurs de l'outil,
- L'adéquation de l'outil aux besoins réels. Ce risque est d'autant élevé que le marché des logiciels dédiés à la Business Intelligence est très large,
- L'implication de la Direction Générale qui est un destinataire plus que probable du tableau de bord,
- L'équilibre entre les indicateurs « techniques » et les indicateurs « orientés clients » : l'objectif du projet est de concevoir un tableau de bord des systèmes d'information et non un tableau de bord informatique,
- Le choix des indicateurs pertinents et non « muets » ou pléthoriques,
- La conception d'un outil en parfaite adéquation avec la stratégie globale de l'entreprise. **[26]**

II.7) Astuces proposées pour la construction d'un tableau de bord :

- Restreindre le nombre des indicateurs.
- Consulter les personnes concernées.
- Bien construire les indicateurs.
- Mettre les indicateurs à l'essai.
- Construire les fiches d'indicateurs.
- Faire figurer les indicateurs par ordre d'importance.
- Tirer profit des couleurs et des graphiques.
- Prévoir une démarche de lecture.
- S'engager à faire évoluer le tableau de bord.
- Éviter d'utiliser le tableau de bord à des fins punitives. **[27]**

II.8) Démarche de sécurisation et tableaux de bord SSI :

Un tableau de bord SSI permet de disposer, aux différents niveaux décisionnels, de pilotage et opérationnels, d'une vision synthétique de la situation de la sécurité, que ce soit dans ses dimensions techniques ou fonctionnelles (couverture des risques, qualité de la politique de sécurité, suivi des audits, des actions et des alertes…). Cette vision renseigne sur l'état et les tendances de la SSI.

Les tableaux de bord peuvent être constitués à partir :

- D'objectifs de sécurité issus d'une analyse de risques.
- De règles de sécurité issues d'une politique de sécurité.
- D'actions de sécurité issues d'un plan d'action.

Dans une démarche structurée de la sécurité des systèmes d'information, les tableaux de bord SSI représentent la suite logique de l'élaboration d'une politique de sécurité et de l'identification des objectifs de sécurité. **[28]**

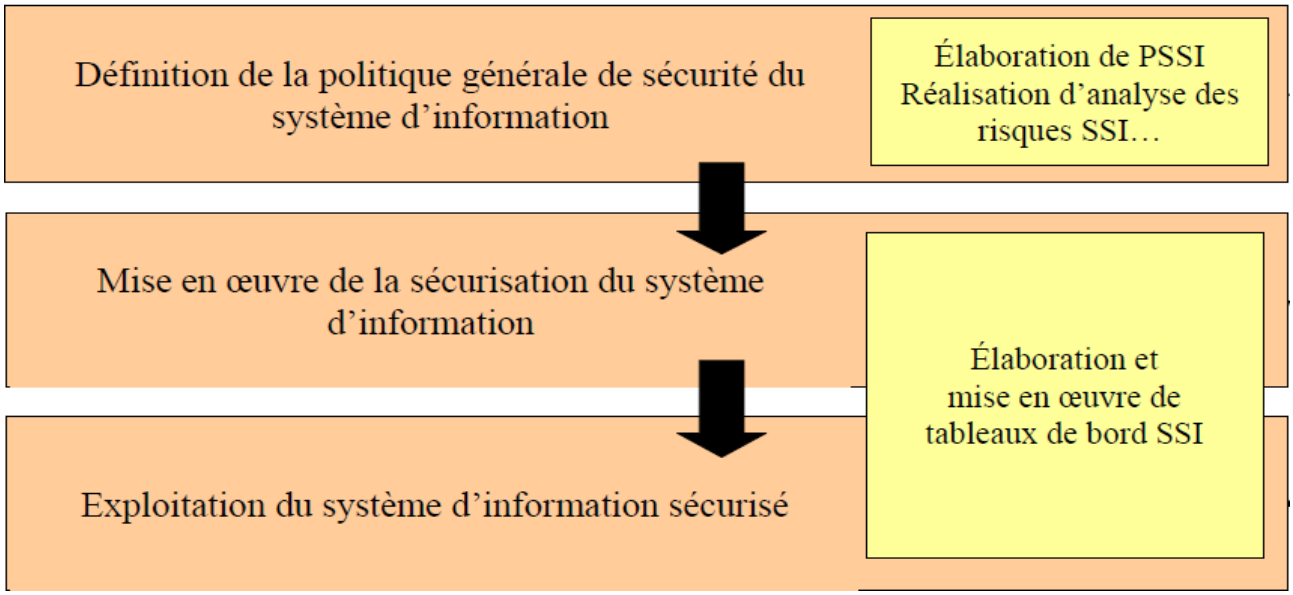


Figure II.8.1 : La place des tableaux de bord SSI dans une démarche sécurité [28].

II.9) Présentation générale de la méthode :

II.9.1) Définition de la méthode:

Les étapes et tâches qui constituent la méthode sont présentées ci-dessous. Le projet de tableaux de bord SSI repose sur une démarche constituée d'une succession d'étapes itératives :

1) **Étape 1 - Prérequis**
2) **Étape 2 - Mise en place du projet Tableaux de bord**
3) **Étape 3 - Élaboration des tableaux de bord**
4) **Étape 4 - Exploitation des tableaux de bord SSI**
5) **Étape 5 - Évolution des tableaux de bord SSI**

Les étapes de constitution de notre tableau de bord SSI selon la méthode sont divisées en cinq, chacune d'entre elles se constitue de plusieurs tâches (chaque tâche a une fiche technique explicative représentée ci-dessus) **[29]** :

Étape 1 - Prérequis

-Tâche 1 : Identification des destinataires des tableaux de bord SSI.

-Tâche 2 : Utilisation prévue des tableaux de bord SSI.

- Tâche 3 : Expression de la périodicité souhaitée des tableaux de bord SSI.

-Tâche 4 : Disponibilité des objectifs de sécurité.

- Tâche 5 : Disponibilité des objectifs de progression de SSI.

- Tâche 6 : Connaissance du système d'information ciblé.

- Tâche 7 : Connaissance des possibilités d'obtention de données sources.

- Tâche 8 : Prise en compte de la dimension budget et moyens.

Étape 2 - Mise en place du projet Tableaux de bord

- Tâche 1 : Identification et mobilisation des acteurs.

- Tâche 2 : Constitution des groupes de travail.

Étape 3 - Élaboration des tableaux de bord

- Tâche 1 : Formalisation des objectifs mesurables.

- Tâche 2 : Sélection des éléments de mesure.

- Tâche 3 : Élaboration des indicateurs.

- Tâche4 : Constitution des tableaux de bord SSI.

- Tâche 5 : Élaboration des procédures d'alimentation.

- Tâche 6 : Validation des tableaux de bord SSI.

Étape 4 - Exploitation des tableaux de bord SSI

- Tâche 1 : Mise en œuvre des tableaux de bord SSI.

Étape 5 - Évolution des tableaux de bord SSI

- Tâche 1 : Suivi des tableaux de bord SSI.

- Tâche 2 : Suivi des modifications du contexte ou des objectifs.

II.10) Fiches techniques de chaque tâche :

II.10.1) Étape 1 – Prérequis :

Tâche 1 - Identification des destinataires des tableaux de bord SSI

Identification des destinataires des tableaux de bord SSI	Étape 1 - Tâche 1
Objectifs de la tâche Identifier la nature des destinataires des tableaux de bord envisagés.	
Éléments en entrée	Éléments en sortie • Liste des destinataires des tableaux de bord SSI et niveaux d'utilisation

Tableau II.10-1 Fiche de synthèse de l'étape 1 tâche 1. [29]

Tâche 2 - Utilisation prévue des tableaux de bord SSI

Utilisation prévue des tableaux de bord SSI	Étape 1 - Tâche 2
Objectifs de la tâche Affiner la qualification des attentes des destinataires des tableaux de bord SSI vis à vis de l'usage qu'ils comptent en faire.	
Éléments en entrée • Liste des destinataires des tableaux de bord SSI et niveaux d'utilisation	Éléments en sortie • Liste des destinataires des tableaux de bord SSI, niveaux d'utilisation et utilisation prévue des tableaux de bord SSI

Tableau II.10-2 : Fiche de synthèse de l'étape 1 tâche 2. [29]

Tâche 3 - Expression de la périodicité souhaitée des tableaux de bord SSI

Expression de la périodicité souhaitée des tableaux de bord SSI	Étape 1 – Tâche 3
Objectifs de la tâche Définir la périodicité de parution souhaitée des tableaux de bord SSI	
Éléments en entrée • Liste des destinataires des tableaux de bord SSI et niveaux d'utilisation	Éléments en sortie • Liste des destinataires des tableaux de bord SSI, niveaux d'utilisation, utilisation prévue et périodicité de parution des tableaux de bord SSI

Tableau II.10-3 : Fiche de synthèse de l'étape 1 tâche 3. [29]

Tâche 4 - Disponibilité des objectifs de sécurité

Disponibilité des objectifs de sécurité	Étape 1 – Tâche 4
Objectifs de la tâche S'assurer que l'on dispose des objectifs de sécurité ou équivalent	
Éléments en entrée • Expression des objectifs de sécurité ou équivalent	Éléments en sortie • Liste des objectifs de sécurité

Tableau II.10-4 : Fiche de synthèse de l'étape 1 tâche 4. [29]

Tâche 5 - Disponibilité des objectifs de progression de SSI

Disponibilité des objectifs de progression de SSI	Étape 1 – Tâche 5
Objectifs de la tâche S’assurer que l’on dispose, s’il y a lieu, d'un « échéancier » de la réalisation des objectifs de sécurité.	
Éléments en entrée • Liste des objectifs de sécurité • Plan d'action SSI ou équivalent	Éléments en sortie • Calendrier de progression de SSI

Tableau II.10-5 : Fiche de synthèse de l’étape 1 tâche 5. [29]

Tâche 6 - Connaissance du système d’information ciblé

Connaissance du système d’information ciblé	Étape 1 – Tâche 6
Objectifs de la tâche S’assurer que le périmètre de SI qui doit être pris en compte par le tableau de bord SSI est parfaitement défini et identifier les sources d’informations correspondantes.	
Éléments en entrée • Documents d’architecture • Coordonnées des services en rapport avec le SI (architecture, exploitation, étude…) • Étude de sécurité (analyse des risques SSI, rapport d'audit…), si disponible	Éléments en sortie • Description synthétique du périmètre fonctionnel et technique du système étudié • Identification des interlocuteurs fonctionnels et techniques du système étudié

Tableau II.10-6 : Fiche de synthèse de l’étape 1 tâche 6. [29]

Tâche 7 - Connaissance des possibilités d'obtention de données sources

Connaissance des possibilités d'obtention de données sources	Étape 1 – Tâche 7
Objectifs de la tâche S'assurer de la disponibilité des éléments techniques du SI ciblé pouvant être utilisés comme sources de données pour les indicateurs techniques, ainsi que des personnes pouvant les mettre à disposition.	
Éléments en entrée • Description synthétique du périmètre fonctionnel et technique du système étudié • Identification des interlocuteurs fonctionnels et techniques du système étudié	Éléments en sortie • Liste des personnes en mesure d'identifier les sources de données utilisables pour constituer des indicateurs

Tableau II.10-7 : Fiche de synthèse de l'étape 1 tâche 7. [29]

Tâche 8 - Prise en compte de la dimension budget et moyens

Prise en compte de la dimension budget et moyens	Étape 1 – Tâche 8
Objectifs de la tâche S'assurer que le projet de mise en place de tableaux de bord SSI pour le système ciblé est bien identifié au niveau budgétaire.	
Éléments en entrée • Documents antérieurs au lancement du projet (étude d'opportunité, marché, appel d'offre, consultation…)	Éléments en sortie • Confirmation du soutien budgétaire du projet de tableaux de bord SSI

Tableau II.10-8 : Fiche de synthèse de l'étape 1 tâche 8. [29]

II.10.2) Étape 2 - Mise en place du projet de tableaux de bord SSI :

Tâche 1 - Identification et mobilisation des acteurs

Identification et mobilisation des acteurs	Étape 2 - Tâche 1
Objectifs de la tâche Identifier tous les acteurs du projet et initier des actions d'information sur les tableaux de bord SSI afin d'expliquer les enjeux du projet et d'impliquer les acteurs.	
Éléments en entrée • Listes des destinataires des tableaux de bord SSI	Éléments en sortie • Annuaire des acteurs du projet • Supports de communication

Tableau II.10-9 : Fiche de synthèse de l'étape 2 tâche 1. [29]

Tâche 2 - Constitution des groupes de travail

Constitution des groupes de travail	Étape 2 - Tâche 2
Objectifs de la tâche Constituer les groupes de travail nécessaires à une définition des tableaux de bord SSI, supportée par les principaux acteurs liés à la sécurité du système étudié, et réaliser la planification du projet	
Éléments en entrée • Annuaire des acteurs du projet	Éléments en sortie • Composition des groupes de travail et attributions • Planning initial du projet • Désignation d'un chef de projet Tableaux de bords SSI

Tableau II.10-10 : Fiche de synthèse de l'étape 2 tâche 2. [29]

II.10.3) Étape 3 - Élaboration des tableaux de bord SSI :

Tâche 1 - Formalisation des objectifs mesurables

Transcription des objectifs de sécurité	Étape 3 - Tâche 1
Objectifs de la tâche Adaptation des objectifs de sécurité de l'organisme à un format utilisable pour les tableaux de bord SSI.	
Éléments en entrée • Objectifs de sécurité identifiés • Objectifs de progression de SSI	Éléments en sortie • Liste des objectifs mesurables avec des valeurs seuils et cibles

Tableau II.10-11 : Fiche de synthèse de l'étape 3 tâche 1. [29]

Tâche 2 - Sélection des éléments de mesure

Sélection des éléments de mesure	Étape 3 - Tâche 2
Objectifs de la tâche Sélectionner les éléments de mesure du système d'information cible les plus à même de remonter des informations pertinentes par rapport aux objectifs.	
Éléments en entrée • Liste des objectifs mesurables avec des valeurs seuils et cibles • Liste des personnes en mesure d'identifier les sources de données utilisables pour constituer des indicateurs	Éléments en sortie • Liste des objectifs mesurables avec des valeurs seuils et cibles, des points-clés et paramètres, des données et sources de données

Tableau II.10-12 : Fiche de synthèse de l'étape 3 tâche 2. [29]

Tâche 3 - Élaboration des indicateurs

Élaboration des indicateurs	Étape 3 - Tâche 3
Objectifs de la tâche Sélection des indicateurs qui seront utilisés dans les tableaux de bord SSI pour suivre l'atteinte des objectifs.	
Éléments en entrée • Liste des objectifs mesurables avec des valeurs seuils et cibles, des points-clés et paramètres, des données et sources de données • Tableaux de bord résultats souhaités à priori	Éléments en sortie • Liste des indicateurs avec leur description

Tableau II.10-13 : Fiche de synthèse de l'étape 3 tâche 3. [29]

Tâche 4 - Constitution des tableaux de bord SSI

Constitution des tableaux de bord SSI	Étape 3 – Tâche 4
Objectifs de la tâche Élaboration des tableaux de bord résultat	
Éléments en entrée • Liste des indicateurs avec leur description • Tableaux de bord résultats à priori	Éléments en sortie • Constitution des tableaux de bord SSI • Fiches descriptives des indicateurs • Maquette des tableaux de bord SSI

Tableau II.10-14 : Fiche de synthèse de l'étape 3 tâche 4. [29]

Tâche 5 - Élaboration des procédures d'alimentation

Élaboration des procédures d'alimentation	Étape 3 - Tâche 5
Objectifs de la tâche Établir des procédures permettant l'alimentation des tableaux de bord SSI de façon récurrente selon une périodicité définie.	
Éléments en entrée • Constitution des tableaux de bord SSI • Fiches descriptives des indicateurs • Maquette des tableaux de bord SSI	Éléments en sortie • Procédures d'alimentation des indicateurs • Procédures d'alimentation des tableaux de bord SSI • Bilan des charges et des coûts induits

Tableau II.10-15 : Fiche de synthèse de l'étape 3 tâche 5. [29]

Tâche 6 - Validation des tableaux de bord SSI :

Validation des tableaux de bord SSI	Étape 3 - Tâche 6
Objectifs de la tâche Validation du projet autant du point de vue fonctionnel et technique que du point de vue des charges associées et des coûts induits.	
Éléments en entrée • Procédures d'alimentation des tableaux de bord SSI • Bilan des charges et des coûts induits • Maquette finalisée des tableaux de bord SSI	Éléments en sortie • Procédures d'alimentation des tableaux de bord SSI validées • Bilan des charges et des coûts induits validé • Maquette des tableaux de bord SSI validée

Tableau II.10-16 : Fiche de synthèse de l'étape 3 tâche 6. [29]

II.10.4) Étape 4 - Exploitation des tableaux de bord SSI :

Tâche 1 - Mise en œuvre des tableaux de bord SSI

Mise en œuvre des tableaux de bord SSI	Étape 4 – Tâche 1
Objectifs de la tâche Édition et exploitation récurrente des tableaux de bord SSI. Cette étape est une étape récurrente qui est réalisée à chaque fois qu'un des tableaux de bord est à éditer selon la périodicité prévue.	
Éléments en entrée • Procédures d'alimentation des tableaux de bord SSI validées • Bilan des charges et des coûts induits validé • Maquette des tableaux de bord SSI validée	Éléments en sortie • Proposition d'actions correctives éventuelles, suite à l'interprétation des tableaux de bord SSI • Éventuellement alarme à la direction

Tableau II.10-17 : Fiche de synthèse de l'étape 4 tâche 1. [29]

II.10.5) Étape 5 - Évolution des tableaux de bord SSI :

Tâche 1 - Suivi des tableaux de bord SSI

<table>
<tr><td>Suivi des tableaux de bord SSI</td><td>Étape 5 – Tâche 1</td></tr>
<tr><td colspan="2">Objectifs de la tâche

Assurer le suivi des tableaux de bord produits afin d’en vérifier régulièrement la qualité et prendre les actions correctives éventuellement nécessaires.</td></tr>
<tr><td>Éléments en entrée

• Tableaux de bord SSI utilisés avec les procédures associées

• Tableaux de bord SSI produits

• Notification d’événements externes : situations exceptionnelles, évolution du cadre de sécurité, évolution du cadre technique…</td><td>Éléments en sortie

• Relevé de décision sur la vérification (audit) et l’évolution des tableaux de bord SSI</td></tr>
</table>

Tableau II.10-18 : Fiche de synthèse de l’étape 5 tâche 1. [29]

Tâche 2 - Suivi des modifications du contexte ou des objectifs

Suivi des modifications du contexte ou des objectifs	Étape 5 – Tâche 2
Objectifs de la tâche Dans le cas d'une modification du cadre de la sécurité du système étudié, vérifier que les tableaux de bord SSI remplissent toujours leur rôle correctement et effectuer les réorientations éventuellement nécessaires. Assurer l'adaptation des tableaux de bord SSI aux évolutions des technologies et du système d'information cible.	
Éléments en entrée • Tableaux de bord SSI utilisés avec les procédures associées • Élément nouveau sur l'efficacité des tableaux de bord ou sur l'évolution du système d'information cible (résultats d'audit des tableaux de bord, résultat d'audit du système d'information, intégration de nouveaux points de sécurité dans les objectifs de sécurité, apparition de nouvelles technologies dans le système d'information…) • Dans le cas de prise en compte d'audit, liste des nouveaux objectifs à intégrer, tels que définis implicitement par les résultats de l'audit	Éléments en sortie • Relevé de décision sur l'évolution des tableaux de bord SSI • Modifications éventuelles apportées aux tableaux de bord SSI et/ou aux procédures associées • Note de lancement éventuelle d'un projet de refonte des tableaux de bord SSI

Tableau II.10-19 : Fiche de synthèse de l'étape 5 tâche 2. [29]

Ces fiches de synthèses donnent un aperçu général sur les différentes tâches pour mieux les cerner.

II.11) Conclusion :

Nous avons abordé dans ce chapitre les concepts de base des tableaux de bord SSI, quelques astuces pour mieux les organiser et les sécuriser, ainsi que la démarche choisie pour élaborer le nôtre que nous allons implémenter dans les chapitres qui suivent.

Chapter 3 :
Les Indicateurs prposés

III.1) Introduction :

Nous allons dans ce chapitre mieux appréhender la norme ISO 27004 qui fournit des réponses bien structurées et normalisées pour mieux mesurer la performance et la sécurité de notre tableau de bord et ainsi présenter les concepts généraux utilisés pour définir les indicateurs qui vont implémenter ce dernier.

III.2) Présentation de la norme ISO/IEC 27004 :

La norme ISO/IEC 27004 fournit des lignes directrices destinées à aider les organisations à évalue les performances de sécurité de l'information et l'efficacité d'un système de management de la sécurité de l'information afin de satisfaire aux exigences de la sécurité Il établit:

1) La surveillance et la mesure des performances de sécurité de l'information.
2) La surveillance et la mesure de l'efficacité d'un système de gestion de la sécurité de l'information (SMSI), y compris ses processus et contrôles.
3) L'analyse et l'évaluation des résultats de la surveillance et de la mesure.

Cette norme s'applique à tous les types et tailles d'organisations.

Cette norme concerne la gestion des indicateurs et leurs utilisations dans le domaine de la sécurité nouvelle.

Objectif :

Mesurer l'efficacité du système de management de la sécurité de l'information et des mesures de sécurité. **[30]**

III.3) Les domaines abordés dans la norme ISO/IEC 27004:

- Présentation du processus de mesurage.
- Rôles et responsabilités.
- Conception des indicateurs.
- Production et mise en forme des indicateurs.
- Analyse et reporting.
- Amélioration du processus de mesurage.
- Une première annexe présente un modèle commenté d'une fiche d'indicateur (cf. Annexe A).
- Une deuxième annexe présente plusieurs exemples d'attributs, de métriques ou d'indicateurs (cf. Annexe B). **[31]**

III.4) Les étapes générales pour mesurer les performances selon la norme ISO/IEC 27004:

III.4.1) Terminologies :

Nous présentons quelques définitions pour mieux comprendre les étapes :

- Attribut : propriété ou caractéristique d'un objet qui peut être distingué quantitativement ou qualitativement par des moyens humains ou automatiques [ISO/IEC 15939 :2007].
- Métrique : ensemble d'éléments permettant de fournir une évaluation qualitative ou quantitative représentative d'une situation.
- Indicateur : résultat de l'application d'un modèle analytique à une ou plusieurs variables en relation avec les critères de décision ou un besoin d'information [ISO/IEC 27004].

III.4.2) Les étapes:

- Mise en place des systèmes et processus métiers de l'entité

- Collecter les paramètres et les variables mesurables : les attributs.

- Concevoir des métriques et les mettre en place.

- Définir les indicateurs perspicaces et essentiels pour la sécurité de l'entreprise.

- Regrouper les indicateurs dans un tableau de bord pour une meilleure visualisation des situations décrites. **[32]**

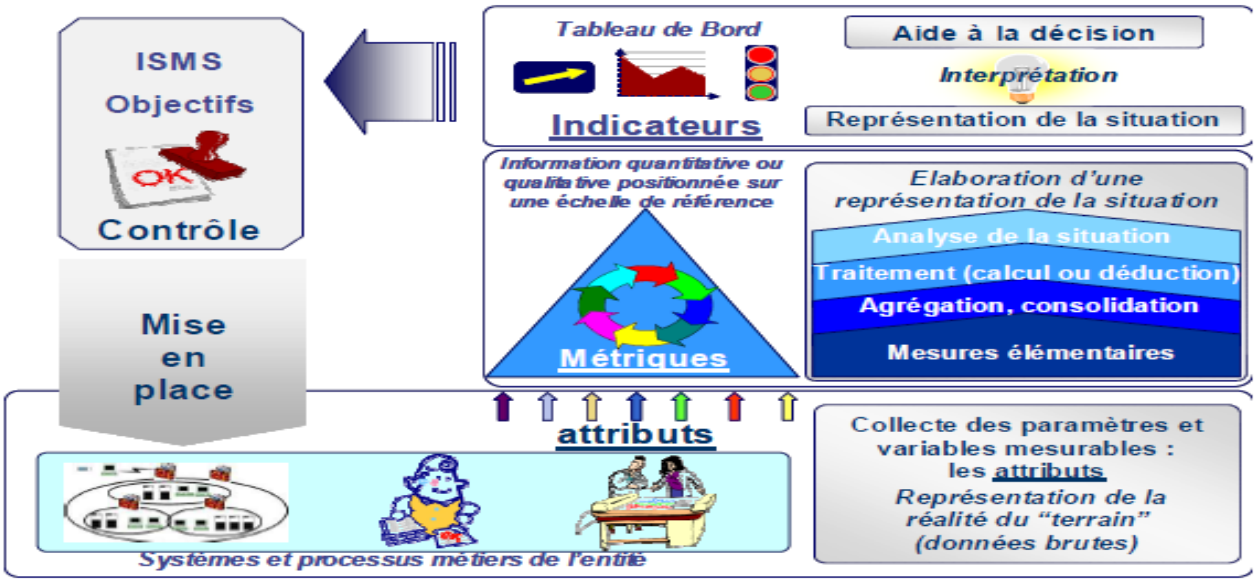


Figure III.4.1 :représentation des étapes d'après le document ISO/IEC 27004. [32]

III.5) Les avantages qu'apporte la norme ISO/IEC 27004 a l'entreprise [33] :

Pour la direction DSI :

- Une vision globale et une approche multi-domaines.
- Un reporting « au bout des doigts » et exploitable pour la direction générale.
- Le contrôle des objectifs et des accords de niveau de service.
- L'auditabilité et la traçabilité des processus.

Pour la sécurité, la DSI et les métiers :

- Une plate-forme de partage de l'information avec toutes les parties concernées (SI, lignes business, RH, juridique, Finances, etc.).
- Approche proactive de la conception de processus.
- Une plus grande autonomie et une délégation multi-domaines.
- Une prestation et solution facilitant le travail d'équipe.
- Moins d'outils de reporting bureautique hétérogènes.
- Une prestation et solution évolutive et modulaire. **[33]**

III.6) Les éléments pour la mise en œuvre des indicateurs :

Afin de satisfaire les objectifs assignés, les indicateurs doivent respecter des conditions particulières et être dotés de qualités spécifiques :

- Etre issus des objectifs retenus dans la politique de sécurité
- Etre aisément quantifiables afin de permettre des comparaisons (entre systèmes ou entre périodes). Il s'agit le plus souvent de pourcentage, de taux, de ratio, de moyenne et/ou de nombres « bruts »
- Les informations nécessaires à l'élaboration de la mesure doivent être faciles à obtenir et/ou collecter. En effet il faut s'assurer que les ressources mises en œuvre pour obtenir les données ne sont pas disproportionnées par rapport à celles concourant à la réalisation du processus mesuré
- S'appuyer sur des processus « stables » et aisément « reproductibles »
- Permettre la mesure des évolutions suite à des actions correctives
- Etre fiables sur la durée et autoriser une analyse des écarts

Ces caractéristiques sont regroupées dans certaines démarches sous l'acronyme « SMART » qui signifie :

- Specific : il correspond à ce qui est analysé et met en avant (la spécificité de l'attribut)
- Measurable : il peut être mesuré et cette mesure est objective
- Attainable : il est obtenu dans des conditions satisfaisantes de coût et de délai
- Repeatable : sa mesure est reproductible

- Time dependent : la mesure dépend de la fenêtre de temps utilisée

Les caractéristiques de la mesure définie dans l'annexe A de la norme ISO/IEC 27004 doivent être définies pour chaque indicateur. **[34]**

III.7) Les différents usages des indicateurs :

III.7.1) Evaluer :

Ces indicateurs peuvent être répartis dans les grandes familles suivantes :

- Les indicateurs « de conformité » : décrivent le niveau d'exigence souhaité (ou constaté) sur une mesure de sécurité.
- Les indicateurs « d'efficacité » : décrivent l'état du fonctionnement de la mesure de sécurité.
- Les indicateurs « d'efficience » : visent à rapprocher l'efficacité de la mesure de sécurité au regard de l'importance des moyens mis en œuvre.

III.7.2) Piloter :

Toute activité (production, projet, processus, etc.) implique la détermination d'indicateur de pilotage. Ces derniers permettent :

- D'apprécier l'avancement correct du projet
- D'évaluer une situation
- De détecter un risque
- De déclencher une alerte

Le choix des indicateurs peut dépendre des objectifs de l'activité (coût, délais, performance, etc.) mais aussi être lié à des processus transverses (management, support, etc.).

Nous pouvons avoir des indicateurs sur différentes échelles de temps : année, mois, semaine, jours, etc.

III.7.3) Communiquer :

Les indicateurs sont aussi utilisés pour communiquer, en interne ou en externe. Leur nature sera différente en fonction des acteurs visés, et de leur objectif de communication (sensibiliser, faire passer des idées, justifier, etc.)

III.7.4) S'autoévaluer :

Cette évaluation peut être réalisée en interne par l'équipe en charge de la fonction comme par l'équipe d'audit ou de contrôle interne.

Elle se situe par rapport à un référentiel interne ou externe ou par rapport à un objectif arbitraire, ou résultant d'une expérience passée et déjà mesurée.

III.7.5) Contribuer à l'obtention d'une certification :

Ces indicateurs servent à :

- Apprécier l'avancement dans le processus de certification
- Obtenir la certification et surtout la conserver

III.7.6) Répondre à un audit :

Les indicateurs servent à informer l'auditeur, à justifier des mesures de sécurité mises en place et des correctifs en cours.

Les indicateurs présentés lors d'audits contribuent à l'analyse de risque et s'apprécient par rapport à un référentiel externe. **[35]**

III.8) Liste des indicateurs proposés :

Après une étude des mesures de l'entreprise ELIT et en suivant la méthode décrite dans la norme ISO/CEI 27004 pour les transformer en indicateurs et la collecte des éléments nécessaires pour leurs mises en œuvre, nous sommes arrivés à proposer les indicateurs suivant pour chacun des 14 domaines de la PSI (vues auparavant dans la norme ISO/CEI 27002) :

N° ind	Domaine de la PSI	Indicateurs
01	Politiques de sécurité de l'information	Taux de conformité à la politique de sécurité de l'information
02	Organisation de la sécurité de l'information	Nombre de vols et/ou de pertes des terminaux mobiles
03	La sécurité des ressources humaines	Pourcentage d'employé non sensibilisés à la sécurité de l'information
04	Gestion des actifs	Classification des systèmes
05	Contrôle d'accès	Pourcentage d'applications couvertes par une politique de contrôle d'accès
06	Cryptographie	Taux de conformité à la politique d'utilisation des mesures cryptographiques
07	Sécurité physique et environnementale	Pourcentage des sites physiques audités
08	Sécurité liée à l'exploitation	Taux de conformité à la politique de sauvegarde
09	Sécurité des communications	Nombre d'engagement de confidentialités signés
10	Acquisition, développement et maintenance des systèmes d'information	Taux de conformité des applications qui répondent à la politique de développement sécurisé
11	Relations avec les fournisseurs	Taux de conformité des prestations de service réalisé par les fournisseurs
12	Gestion des incidents liés à la sécurité de l'information	Nombre d'incidents signalés
13	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	Nombre d'incidents causant l'indisponibilité des activités classées critiques
14	Conformité	Nombre d'applications possédants le droit de propriété intellectuelle

Tableau III.8-1 : tableau représentant la liste des indicateurs propos

III.9) Fiche technique de chaque indicateur :

Afin de mieux analyser les indicateurs et connaitre les métriques et durée de chacun d'eux, il se doit d'avoir une fiche technique détaillée :

III.9.1) Domaine 1 : Politiques de sécurité de l'information

Nous allons calculer dans ce domaine le taux de conformité à la politique de sécurité de l'information pour chaque filiale de l'entreprise et les représenter dans un graphique en bâton dans notre tableau de bord, si une des filiales ne sera pas conforme à la PSI de l'entreprise et dépasse le seuil de tolérance une alerte sera déclenchée.

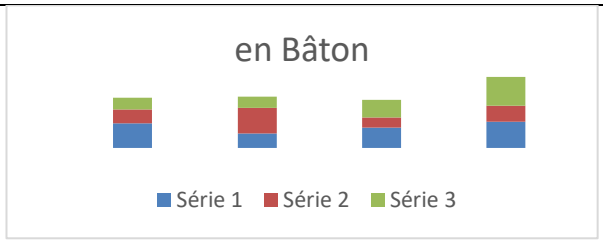
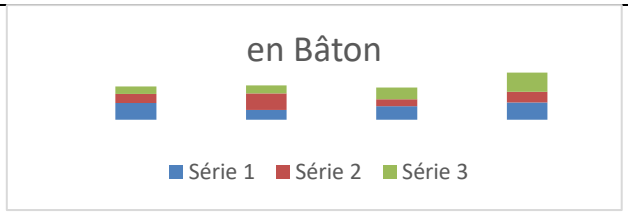
Nom de l'indicateur	Taux de conformité à la politique de sécurité de l'information
Type	Stratégique
Objectif	Vérifier si les procédures de sécurité sont correctement appliquées par la DSI et les métiers notamment en matière de protection et de traçabilité des données
Source	administrative
Calcul	Nb d'audits Effectués avec succès/ nb d'audits effectués
Périodicité	annuelle
Seuil de tolérance	<50%
Représentation graphique	

Tableau III.9-1: fiche technique de l'indicateur numéro 1

III.9.2) Domaine 2 : Organisation de la sécurité de l'information

Nous allons calculer dans ce domaine le nombre de vols et/ou de pertes des terminaux mobiles pour chaque filiale de l'entreprise représenté en graphique bâton dans notre tableau de bord, si un

Nom	Nombre de vols et/ou de pertes des terminaux mobile
Type	opérationnel
Objectif	Permet de sécuriser l'accès à l'appareil, paramétrer certaines options de sécurité, vérifier la conformité pour empêcher l'accès aux ressources de l'organisation comme la messagerie par les terminaux non conformes.
Source	Interne (entreprise) et externe (personnes externes)
Calcul	Nombre de terminaux mobiles volés
Périodicité	Mensuelle
Seuil de tolérance	1 (1 terminal volé)
Représentation graphique	

seul terminal mobile manquera à l'un des employés, des données pourront être perdues et la sécurité de l'entreprise sera en péril, une alerte serait donc déclenchée.

Tableau III.9-2: fiche technique de l'indicateur numéro 2

III.9.3) Domaine 3 : La sécurité des ressources humaines

Nous allons calculer dans ce domaine le pourcentage des employés qui n'ont pas été sensibiliser pour contribuer à la sécurité de l'entreprise, ce pourcentage sera représenté en graphique camembert dans notre tableau de bord, si un certain pourcentage d'employés n'a pas suivi la formation de sensibilisation une alerte sera déclenchée.

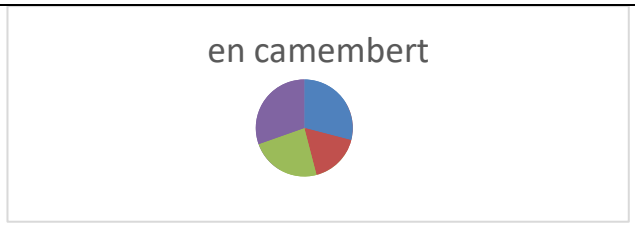
Nom	Pourcentage d'employé non sensibilisés à la sécurité de l'information
Type	Stratégique
Objectif	Sensibiliser un maximum de personnel sur la sécurité afin d'atteindre un ratio de protection de 100% surtout pour les salariés intervenant sur des systèmes critiques
Source	Interne (personnels de l'entreprise)
Calcul	Nb personnes n'ayant pas suivi une formation dédiée SSI / nb personnes concernées (totale)
Périodicité	Annuelle
Seuil de tolérance	>30%
Représentation graphique	

Tableau III.9-3: fiche technique de l'indicateur numéro 3

III.9.4) Domaine 4: Gestion des actifs

Dans ce domaine notre indicateur sera la classification des systèmes, il nous permettra de déterminer les actifs informatique critiques pour chaque filiale et si les objectifs de sécurité sont bien au point, nous aurons un graphique en bâton pour le représenté dans notre tableau de bord, si un certain pourcentage de classification ne sera pas respecté une alerte sera déclenchée.

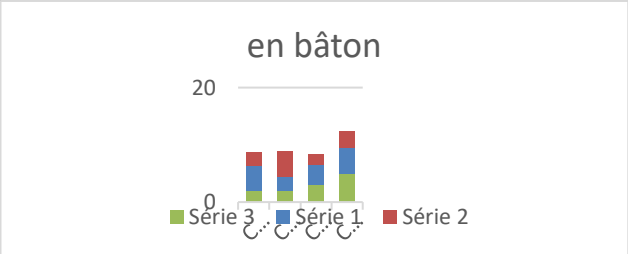
Nom	Classification des systèmes
Type	Stratégique
Objectif	permet de déterminer la criticité des actifs informatiques pour l'entreprise , en fonction des 3 objectifs de sécurité de l'information soit la disponibilité, l'intégrité et la confidentialité
Source	Interne (actifs informatique de l'entreprise)
Calcul	Nombre de systèmes classifiés/Nombre total de systèmes
Périodicité	Annuelle
Seuil de tolérance	<30%
Représentation graphique	

Tableau III.9-4 : fiche technique de l'indicateur numéro 4

III.9.5) Domaine 5: Contrôle d'accès

Dans ce domaine nous allons calculer le pourcentage d'applications couvertes par une politique de contrôle d'accès pour chaque filiale de l'entreprise, le graphique sera en bâton dans notre tableau de bord, si un certain pourcentage n'est pas contrôler une alerte sera déclenchée.

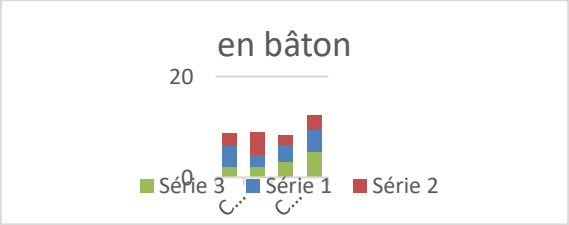
Nom	Pourcentage d'applications couvertes par une politique de contrôle d'accès
Type	Stratégique
Objectif	elle consiste à soumettre l'entrée de l'établissement ou, de locaux à l'intérieur d'une entreprise, à une autorisation d'accès, cette autorisation d'accès a pour but de protéger des personnes, des biens ou des informations.
Source	Administrative
Calcul	Nb d'applications sensibles ou non couvertes par une politique d'accès / habilitation
Périodicité	Annuelle
Seuil de tolérance	>50%
Représentation graphique	

Tableau III.9-5 : fiche technique de l'indicateur numéro 5

III.9.6) Domaine 6: Cryptographie

Nous savons que la cryptographie est le point fort de la sécurité, nous allons donc calculer dans ce domaine le taux de conformité à la politique d'utilisation des mesures cryptographiques pour chaque filiale de l'entreprise qui sera représenté en bâton dans notre tableau de bord, si un certain pourcentage de mesures cryptographiques n'est pas pris en charge une alerte sera déclenchée.

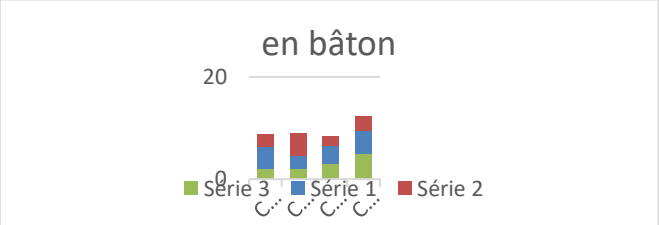
Nom	Taux de conformité à la politique d'utilisation des mesures cryptographiques
Type	Stratégique
Objectif	Protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des algorithmes utilisant des clés de chiffrement. il faut les utiliser aussi pour protéger les flux d'information liés à des services sensibles
Source	Administrative
Calcul	Nb de mesures cryptographiques effectués avec succès/ nr totale de mesures cryptographiques effectués
Périodicité	6 mois
Seuil de tolérance	<20%
Représentation graphique	

Tableau III.9-6 : fiche technique de l'indicateur numéro 6

III.9.7) Domaine 7: Sécurité physique et environnementale

Pour mieux choisir l'emplacement dans nos entreprises ou filiale, il faut bien étudier les terrains et construire des bâtiments sécurisés dans des endroits surs afin de garantir au mieux la sécurité, pour cela dans ce domaine nous allons avoir le pourcentage des sites physiques audités pour chaque filiale représentée en bâton dans notre tableau de bord.

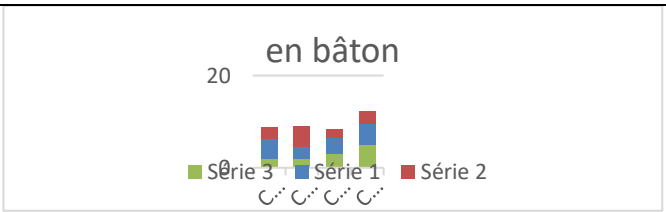
Nom	Pourcentage des sites physiques audités
Type	Opérationnel
Objectif	empêcher tout accès physique non-autorisés, dommage ou intrusion dans le périmètre de l'entreprise, la dégradation, le vol, et l'atteinte à l'intégrité des actifs de l'entreprise
Source	Environnementale
Calcul	Nombre de sites audités / nombre totale de sites
Périodicité	Mensuelle
Seuil de tolérance	0 (aucun audit d'une filiale pendant 1 an)
Représentation graphique	

Tableau III.9-7: fiche technique de l'indicateur numéro 7

III.9.8) Domaine 8: Sécurité liée à l'exploitation

Dans ce domaine nous allons calculer le taux de conformité à la politique de sauvegarde pour chaque filiale, ainsi nous allons protéger nos données et les sauvegarder en toute sécurité, le graphique sera représenté en bâton dans notre tableau de bord, si un certain pourcentage de sauvegarde de données n'est pas respecté, une alerte sera déclenchée.

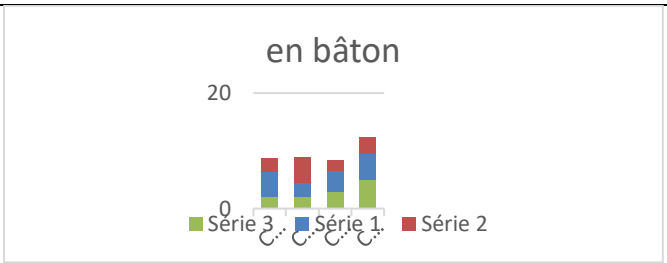
Nom	Taux de conformité à la politique de sauvegarde
Type	Stratégique
Objectif	Protéger contre la pertes de données et d'informations
Source	Administrative
Calcul	Nb de données non sauvegarder avec succès / nb totale de données
Périodicité	4 Mois
Seuil de tolérance	>20%
Représentation graphique	

Tableau III.9-8: fiche technique de l'indicateur numéro 8

III.9.9) Domaine 9: Sécurité des communications

Afin que la communication accords interentreprises soient confidentiels et sécurisés nous allons calculer dans ce domaine le pourcentage des accords de confidentialités signés par l'entreprise, le graphique sera présenté en camembert dans notre tableau de bord, si un certain pourcentage de confidentialité n'est pas respecté une alerte sera déclenchée.

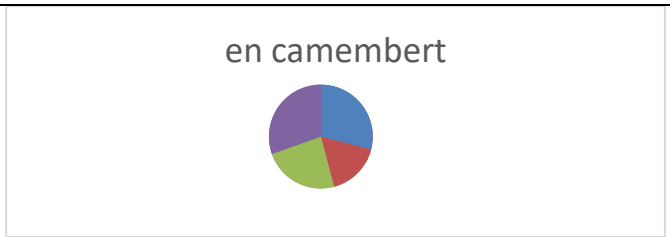
Nom	Pourcentage des accords de confidentialités signés
Type	Stratégique
Objectif	Cerner les engagements réciproques des parties ainsi que les sanctions en cas de violation de l'obligation contractuelle
Source	Administrative
Calcul	Nombre d'engagement de confidentialités signés/ Nombre d'employés de la société
Périodicité	Annuelle
Seuil de tolérance	< 30%
Représentation graphique	

Tableau III.9-9: fiche technique de l'indicateur numéro 9

III.9.10) Domaine 10: Acquisition, développement et maintenance des systèmes d'information

Toutes entreprise se doit de s'approprier les meilleures applications sécurisées afin de garder son ampleur, dans ce domaine nous allons calculer le taux de conformité des applications qui répondent à la politique de développement sécurisé dans toute l'entreprise, le graphique sera donc représenté en bâton dans notre tableau de bord car plusieurs filiales peuvent utiliser les mêmes applications, ainsi si un certain taux n'est pas respecté une alerte sera déclenchée.

Nom	Taux de conformité des applications qui répondent à la politique de développement sécurisé
Type	Opérationnel
Objectif	Garantir la conformité de l'application avec un ensemble spécifique de critères de sécurité
Source	Développement interne
Calcul	Nb d'applications développées avec succès / nb d'applications totale
Périodicité	Mensuelle
Seuil de tolérance	<30%
Représentation graphique	

Tableau III.9-10 : fiche technique de l'indicateur numéro 10

III.9.11) Domaine 11: Relations avec les fournisseurs

Pour satisfaire les clients, dépasser la concurrence et s'approprier les meilleurs fournisseurs pour l'entreprise, nous allons calculer dans ce domaine le Taux de conformité des prestations de service réalisé par les fournisseurs pour chaque filiale de l'entreprise, le graphique sera en bâton dans notre tableau de bord, si le taux de prestations est inférieur à 30% une alerte sera déclenchée.

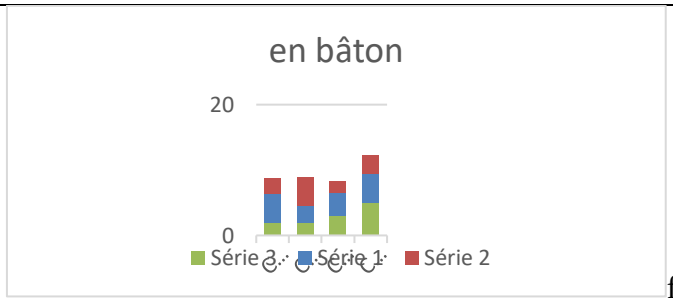
Nom	Taux de conformité des prestations de service réalisé par les fournisseurs
Type	Stratégique
Objectif	Contrôler et assurer la bonne conformité de la commande ainsi qu'améliorer la satisfaction des utilisateurs à court et long terme.
Source	Interne et externe
Calcul	Nb de prestations réalisées avec succès / nb de prestations totale
Périodicité	Annuelle
Seuil de tolérance	<30%
Représentation graphique	 filiale

Tableau III.9-11: fiche technique de l'indicateur numéro 11

III.9.12) Domaine 12 : Gestion des incidents liés à la sécurité de l'information

Dans ce domaine nous allons calculer le nombre d'incidents signalés par filiale, quel que soit les incidents de travail, les congés, les incidents matériels, etc. si un certain nombre d'incidents est dépassé, une alerte sera déclenchée.

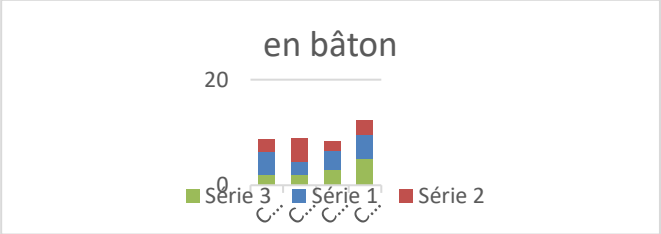
Nom	Nombre d'incidents signalés
Type	opérationnel
Objectif	Aide à la classification et analyse des incidents
Source	interne
Calcul	Nombre d'incidents signalés
Périodicité	mensuelle
Seuil de tolérance	50
Représentation graphique	

Tableau III.9-12 : fiche technique de l'indicateur numéro 12

III.9.13) Domaine 13: Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Certains incidents peuvent causer l'arrêt de certaine activités critiques au seins de l'entreprise, pour cela nous allons calculer dans ce domaine le Nombre d'incidents causant l'indisponibilité des activités classées critiques pour chaque filiale, le graphique est représenté en bâton dans le tableau de bord, si un certain nombre d'incidents est atteint, une alerte sera déclenchée.

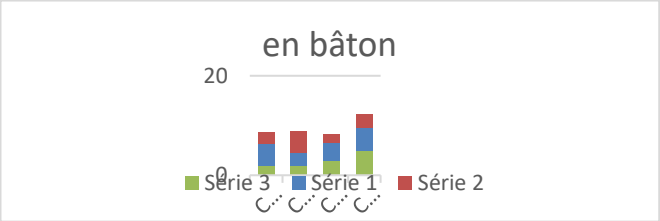
Nom	Nombre d'incidents causant l'indisponibilité des activités classées critiques
Type	Opérationnel
Objectif	Prévention et d'anticipation pour affronter un danger ou un risque, il renforce la résilience de l'entreprise. Il servira à coordonner les différentes actions à entreprendre, à réagir rapidement en rassemblant les bonnes personnes.
Source	Interne et externe
Calcul	Nombre d'incidents causant l'indisponibilité des activités classées critiques
Périodicité	Mensuelle
Seuil de tolérance	5
Représentation graphique	

Tableau III.9-13 : fiche technique de l'indicateur numéro 13

III.9.14) Domaine 14: Conformité

Pour garantir la performance et la sécurité des applications au seins de l'entreprise, il faut qu'elles aient le droit de propriété intellectuelle, afin d'éviter tout risque venu de l'extérieur. Dans ce domaine nous allons calculer le Pourcentage d'applications possédants le droit de propriété intellectuelle pour chaque filiale de l'entreprise, le graphique est représenté en bâton dans le tableau de bord, si un certain pourcentage d'application ne possède pas le droit de propriété intellectuelle, une alerte sera déclenchée.

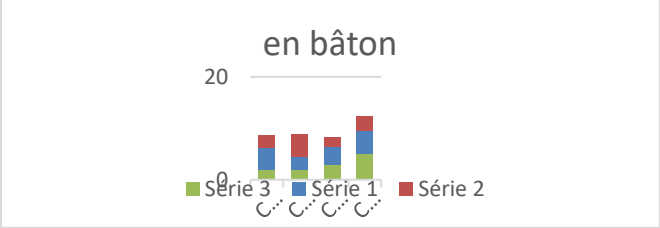
Nom	Pourcentage d'applications possédants le droit de propriété intellectuelle
Type	Stratégique
Objectif	S'assurer de l'exécution par l'établissement de ses obligations légales et de son respect des bonnes pratiques et des règles professionnelles et déontologiques.
Source	Administrative
Calcul	Nombre d'applications possédants le droit de propriété intellectuelle / nombre totale d'applications
Périodicité	Annuelle
Seuil de tolérance	<20%
Représentation graphique	

Tableau III.9-14: fiche technique de l'indicateur numéro 14

III.10) Conclusion :

Nous sommes arrivés dans ce chapitre après une étude approfondie de la norme ISO/IEC 27004, à transformer des métriques en différents indicateurs de sécurité, chacun adapté à un domaine précis de la PSI et à remplir leurs fiches techniques tout en respectant les principes de sécurité de l'information.

Chapter 4 : Conception

IV.1) Introduction :

Il y a plusieurs démarches en génie logiciel tel que UML qui est conçue pour modéliser le système d'information, donc pour arriver à développer correctement, il faut d'abord réaliser tous les diagrammes nécessaires.

IV.2) Description du projet :

Afin d'arriver à créer le tableau de bord sécurité idéal et un suivie exacte de la PSI, et d'avoir une vue réelle sur l'avancement du projet et la mise en place des mesures de sécurité, nous présentons notre démarche comme suit :

- Etudier les normes liées à la sécurité de l'organisme (dans notre cas c'est les normes ISO/IEC 27002 et ISO/IEC 27004).
- Identifier et détailler les domaines de la PSI (à partir de la norme ISO/IEC 27002).
- Créer les indicateurs de performance pertinents est indispensables (méthode utilisée à partir de la norme ISO/IEC 27004).
- Découper les indicateurs en deux parties : stratégiques et opérationnels.
- Adapter chaque indicateur a son domaine.
- Implémenter le tableau de bord sécurité.

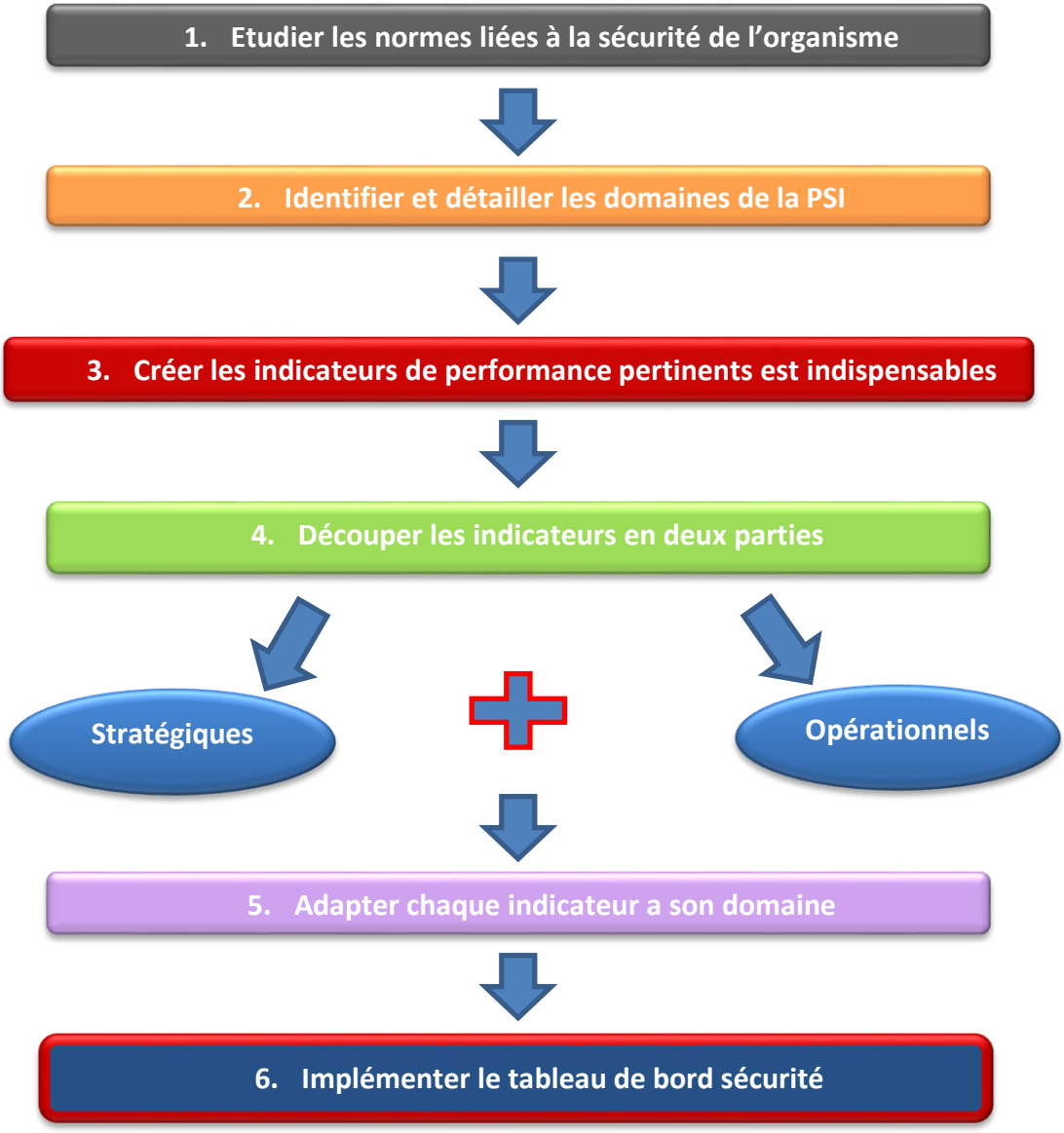


Figure IV.2-1 : la démarche de notre solution

IV.3) Conception :

Avant d'entamer l'implémentation, la conception est la dernière étape de notre projet.

Dans cette partie nous allons identifier deux diagrammes:

● Les diagrammes de cas d'utilisations représentent un intérêt pour l'analyse des besoins métier ce qui nous permettra de démarrer l'analyse orientée objet et identifier les classes candidates.

● Un diagramme de classes est une collection d'éléments de modélisations statiques (classes, paquetages...), qui montre la structure d'un modèle. Les classes sont liées entre elles par des associations. Une association permet d'exprimer une connexion sémantique bidirectionnelle entre deux classes. **[36]**

IV.3.1) Conception des couches:

Cette phase consiste à enrichir la description du procédé, de détails d'implémentation afin d'aboutir à une description très proche d'un programme. Nous allons modéliser toute la nouvelle approche en diagramme de cas d'utilisation, et de classes.

IV.3.2) Diagramme de cas d'utilisation:

Le diagramme suivant représente le cas d'utilisation de notre tableau de bord. Il décrit le comportement du système du point de vue admin et employés

l'admin : il a les fonctionalitées suivantes :

- La gestion du tableau de bord
- Il s'occupe de la gestion des employés (ajout avec points d'accès, modifier des informations personnelles, supprimer des employés).
- Pour l'efficacité de notre tableau de bord sécurité, l'admin doit créer les bons indicateurs (avec possibilité d'ajout, modification et suppression), les découper en deux sessions pour une meilleure gestion et impression.
- Affecter chaque indicateur a un domaine bien précis de la PSI.
- Il gère les droits d'accès en enlevant toutes les permissions aux employer (ajout, suppression et modification des indicateurs) sauf la saisie des nouvelles valeurs.
- Il reçoit des alertes de sécurité en cas ou un indicateur dépasse son seuil de tolérance ou bien une notification de mise à jour.
- Il a le bilan du déroulement de l'application.

Concernant **l'employé** :

- il accède donc au tableau de bord
- il va visionner tous types d'indicateurs
- il saisit les nouvelles valeurs qui vont apporter la différence dans les graphiques et peut être même déclencher
- il recoit les mâmes alertes de sécurité et notifications de mise à jour .

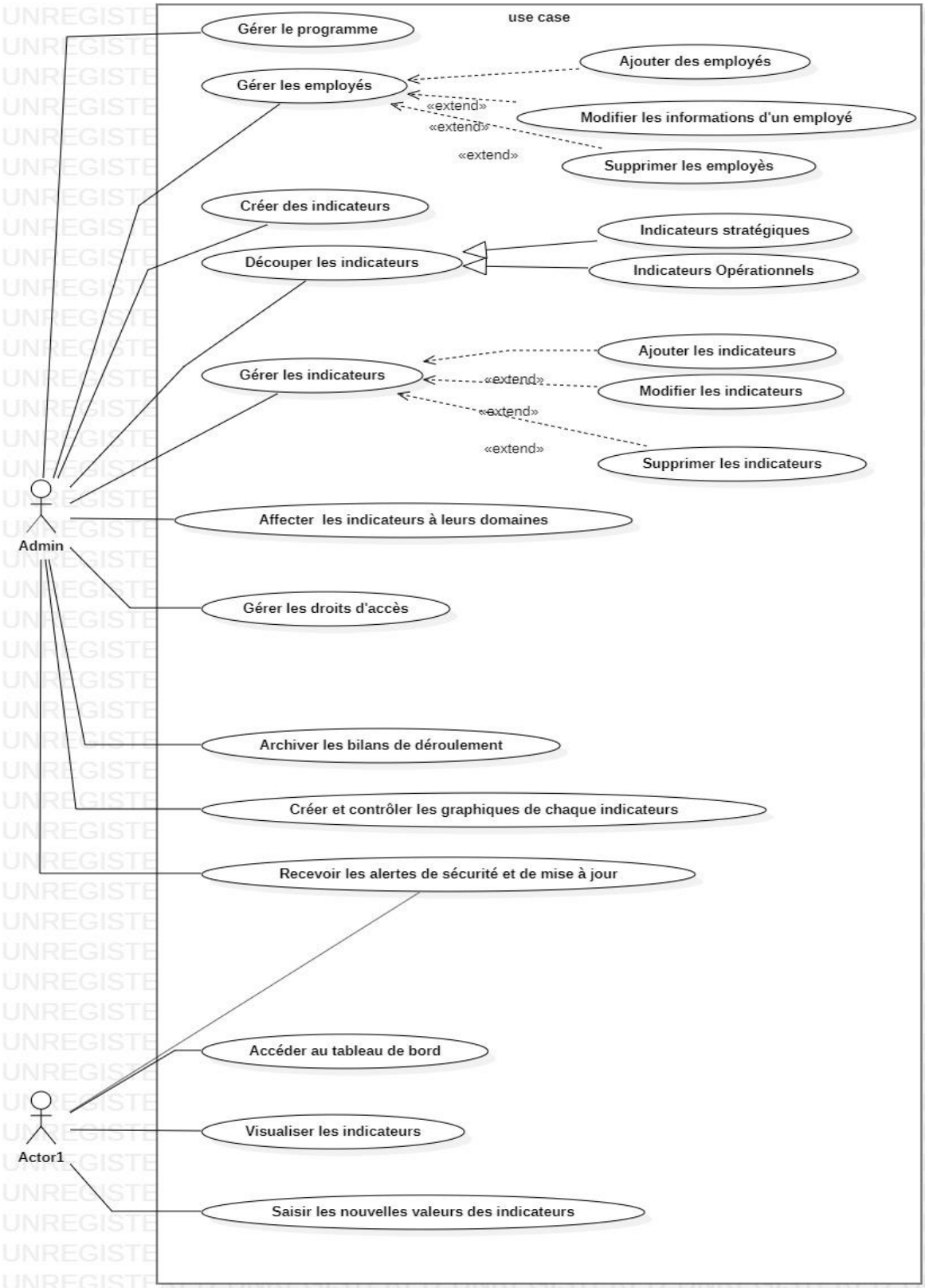


Figure IV.3-1: diagramme de cas d'utilisation

IV.3.3) Diagramme de classe :

Pour décrire les associations entre les classes et afin de déterminer les dépendances entre elles, nous présentons le diagramme de classe suivant :

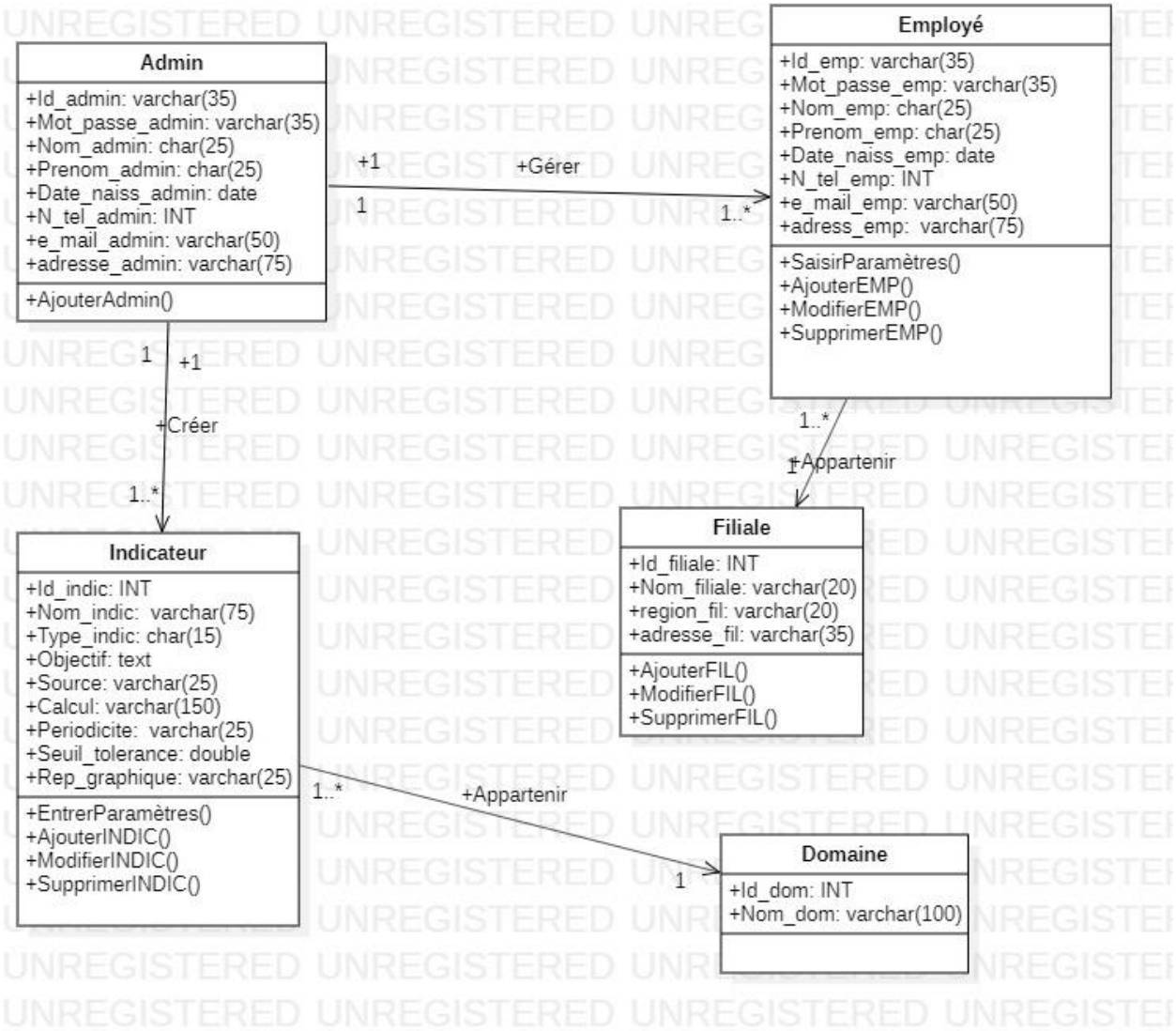


Figure IV.3-2: Figure : Diagramme de classe

IV.4) Conclusion :

Dans ce chapitre, nous avons identifié les diagrammes de cas d'utilisation, et de classes pour faciliter la réalisation de notre prototype.

Dans le chapitre suivant nous montrerons les étapes, plus en détails, que nous avons suivies pour implémenter et réaliser notre solution.

Chapter 5 : Implémentation

V.1) Introduction :

Après analyse et conception de notre application, nous entamons la phase la plus importante l'implémentation.

Le choix des outils de développement influe énormément sur le coût en temps de programmation, ainsi que sur la flexibilité du produit à réaliser. Cette phase consiste à transformer le modèle conceptuel établi précédemment en des composants logiciels formant notre prototype.

Dans ce chapitre, nous allons commencer par la description de l'environnement de travail, présenter les outils contribuant à notre réalisation, présenter l'organigramme d'interaction puis à dégager et à élaborer les composants de notre système.

V.2) Environnement de travail :

L'environnement de travail se constitue de deux parties : matériel et logiciel.

V.2.1) Environnement matériel :

Notre environnement matériel est caractérisé par :

- Système d'exploitation : Windows 10 Professionnel 64bits
- Processeur: Intel(R) Core(TM) i5-6200U CPU @ 2.30GHz 2.40 GHz, processeur x64
- Mémoire RAM : 4,00 Go

V.2.2)Environnement logiciel :

Notre environnement matériel est constitué de :

V.2.2.1) **Langage de développement :**

JAVA :

Java est un langage de programmation orienté objet développé par Sun Microsystems (aujourd'hui racheté par Oracle) Le choix du langage JAVA pour le développement de ce projet a été motivé par les point suivants :

- ✓ **Orienté objet :** permet l'encapsulation, le polymorphisme, et l'héritage, et qui vont nous aider à bien organiser et structurer l'application.
- ✓ **Portabilité :** En effet un programme développé en java peut s'exécuter sur n'importe quelle machine c'est-à-dire tout environnement (Windows, Unix et Mac), à condition bien sûr que celle-ci dispose d'une machine virtuelle java. **[37]**
- ✓

- ✓ **Distribué :** Java possède une importante bibliothèque de routines permettant de gérer les protocoles TCP/IP tels que HTTP et FTP. Les applications Java peuvent charger et accéder à des sites sur Internet via des URL avec la même facilité qu'elles accèdent à un fichier local sur le système.
- ✓ **Fiabilité :** Java a été conçu pour que les programmes qui l'utilisent soient fiables sous différents aspects. Sa conception encourage le programmeur à traquer préventivement les éventuels problèmes, à lancer des vérifications dynamiques en cours d'exécution et à éliminer les situations génératrices d'erreurs.
- ✓ **Sécurité :** Java a été conçu pour être exploité dans des environnements serveur et distribués. Dans ce but, la sécurité n'a pas été négligée. Java permet la construction de systèmes inaltérables et sans virus. **[38]**

Langage SQL :

Signifie « Structured Query Language » c'est-à-dire « Langage d'interrogation structuré », En fait SQL est un langage complet de gestion de base de données relationnelle. Il permet :

- ✓ La création de base et des tables.
- ✓ L'ajout d'enregistrements sous forme de lignes.
- ✓ L'interrogation de la base.
- ✓ La mise à jour.
- ✓ Le changement de structure de la table: ajout, suppression de colonnes.
- ✓ La gestion de droits d'utilisateurs de la base.
- ✓ SQL permet l'interaction avec le serveur et les informations qu'il héberge en soumettant une commande au SGBD sous la forme d'une requête. **[39]**

V.2.2.2) **Outils de développement :**

Netbeans IDE 8.2:

NetBeans est un environnement de développement intégré (IDE) pour Java, placé en open source par Sun en juin 2000 sous licence CDDL (Common Development and Distribution License). En plus de Java, NetBeans permet également de supporter différents autres langages, comme Python, C, C++, XML et HTML. Il comprend toutes les caractéristiques d'un IDE moderne (éditeur en couleur, projets multi-langage, refactoring, éditeur graphique d'interfaces et de pages web).

NetBeans est disponible sous Windows, Linux, Solaris (sur x86 et SPARC), Mac OS X et Open VMS.

NetBeans est lui-même développé en Java, ce qui peut le rendre assez lent et gourmand en ressources mémoires. **[40]**

NetBeans IDE propose des outils de première classe pour le développement d'applications Web, d'entreprise, de bureau et mobiles Java. Il est systématiquement le premier environnement IDE à prendre en charge les dernières versions de JDK, Java EE et JavaFX. Il fournit des aperçus intelligents pour aider à comprendre et à gérer vos applications, y compris une prise en charge complète des technologies populaires telles que Maven.

Avec ses fonctionnalités de développement d'applications de bout en bout, l'amélioration constante de Java Editor et ses améliorations en continu en termes de performances et de vitesse, NetBeans IDE établit la norme en matière de développement d'applications avec des technologies de pointe prêtes à l'emploi. **[41]**

JavaFX:

JavaFX est une technologie crée par Sun Microsystems qui appartient désormais à Oracle. Avec l'apparition de Java 8 en mars 2014, JavaFX devient la bibliothèque de création d'interface graphique officielle du langage Java, pour toutes les sortes d'application (applications mobiles, applications sur poste de travail, applications Web), le développement de son prédécesseur Swing étant abandonné (sauf pour les corrections de bogues). JavaFX contient des outils très divers, notamment pour les médias audio et vidéo, le graphisme 2D et 3D, la programmation Web, la programmation multi-fils etc.

Le SDK de JavaFX étant désormais intégré au JDK standard Java SE, il n'y a pas besoin de réaliser d'installation spécifique pour JavaFX. **[42]**

Caractéristiques du JAVAFX :

- Types: String, Number, Integer, Boolean, Void, Null, Duration.
- On ne déclare pas le type, il est impliqué par ce qui est assigné. On utile le mot-clé var ou def.
- Les opérateurs sont ceux de Java.
- Toute chose est une expression.
- Un objet est défini par un littéral selon la syntaxe d'un tableau comme en JavaScript.
- Les symboles {} ont des usages multiples. Ils servent à grouper un contenu, à insérer une variable dans une chaîne (PHP utilise directement la variable avec son préfixe $). A concaténer des chaînes.
- Le même chose peut être écrite de façon équivalente sous une forme déclarative et une forme procédurale.
- Il peut utiliser les classes Java préexistantes. **[43]**

WampServer :

WampServer (anciennement WAMP5) est une plateforme de développement Web de type WAMP, permettant de faire fonctionner localement (sans se connecter à un serveur externe) des scripts PHP. WampServer n'est pas en soi un logiciel, mais un environnement comprenant deux

serveurs (Apache et MySQL), un interpréteur de script (PHP), ainsi que phpMyAdmin pour l'administration Web des bases MySQL.

Il dispose d'une interface d'administration permettant de gérer et d'administrer ses serveurs au travers d'un tray icon (icône près de l'horloge de Windows).

La grande nouveauté de WampServer 2 réside dans la possibilité d'y installer et d'utiliser n'importe quelle version de PHP, Apache ou MySQL en un clic. Ainsi, chaque développeur peut reproduire fidèlement son serveur de production sur sa machine locale. **[44]**

PhpMyAdmin :

PhpMyAdmin est un logiciel gratuit écrit en langage PHP qui sert à gérer l'administration de MySQL en utilisant l'internet. Ce logiciel a été créé en 1998 par T. Ratschiller. Son nom dérive de PHP (le langage utilisé), MySQL (la base de données gérée) et administration (l'activité pratiquée par le logiciel). PhpMyAdmin a été traduit en 72 langues pour permettre une utilisation mondiale. La dernière version est la phpMyAdmin 4.1.7 lancée en février 2014.

PhpMyAdmin a une grande variété d'utilisation. Ses utilisations les plus courantes sont :

- gestion de base de données, tables, colonnes, index, etc.

- gestion d'utilisateurs, permissions, et privilèges de certains utilisateurs.

La gestion de base de données inclus plusieurs autres sous-utilisations comme créer, consulter ou modifier des tables. Par ailleurs, on peut exécuter avec phpMyAdmin n'importe quelle requête MySQL. **[45]**

MariaDB (Data Base) :

MariaDB est un Système de Gestion de Base de Données (SGBD) disponible sous licence GPL. Ce système est un fork de MySQL, ce qui signifie que c'est un nouveau logiciel créé à partir du code source de MySQL.

Sachant que MySQL a fini par devenir un projet de l'entreprise Oracle, l'informaticien Michael Widenius qui est le principal développeur de MySQL décide de créer MariaDB dans le but de remplacer MySQL et d'assurer une interopérabilité avec celui-ci.

On l'a choisie pour être notre Base de données du projet. **[46]**

V.2.3) Sécurité de l'application :

Pour mieux protéger notre prototype informatique nous avons ajouté quelques options de sécurité :

V.2.3.1) **Fichier LOG (fichier journal) :**

Les fichiers logs tracent tous les événements qui arrivent pendant l'activité d'un système. Ils peuvent contenir la preuve en détail de toute activité exceptionnelle, suspecte ou non désirée. Les fichiers logs issus des différents composants d'un réseau peuvent indiquer si la sécurité du réseau est compromise ou en voie de compromission. Ils sont la seule information que l'attaquant laisse derrière lui après son introduction dans un réseau, ils représentent l'empreinte de l'attaquant. Lors d'une attaque, l'information contenue dans les fichiers logs peut être vérifiée pour définir les traces de l'attaque et aboutir à une preuve accusatrice. **[47]**

Pour mieux assurer notre application nous avons deux types de fichiers log :

- MariaDB log : il est généré automatiquement par notre base de données MariaDB, il suit toute trace des actions qui se passent dans notre base de données, si quelqu'un d'autre s'introduit à notre système on pourra détecter les actions qu'il a faites.

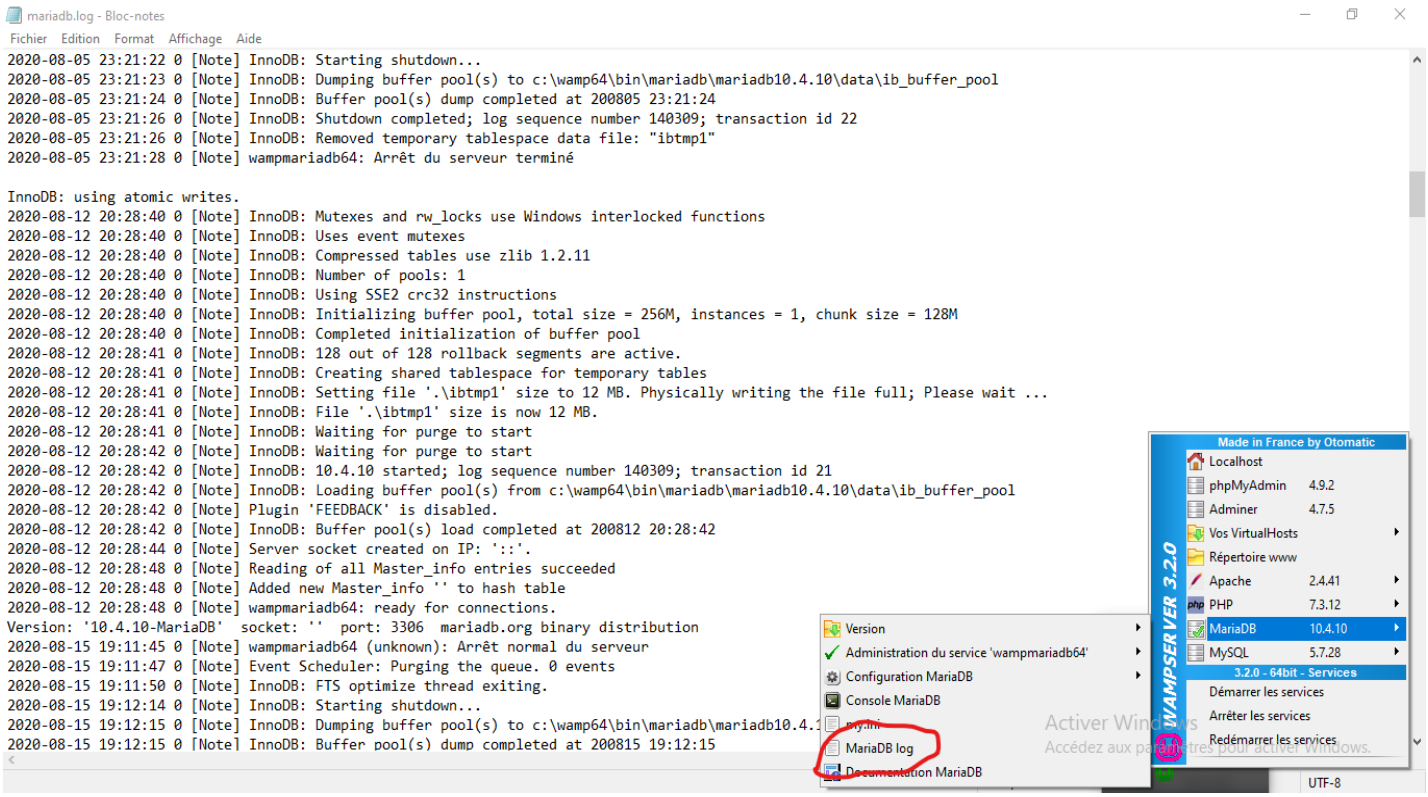


Figure V.2-1: Aperçus du fichier journal de notre base de données MariaDB

- Application log : concernant le fichier journal de notre application, dans l'outil de développement Netbeans il existe une API java.util.logging qui contient les classes pour gérer simplement un fichier journal (fichier log) dans lequel notre

applications va laisser une trace de l' exécution. Les lignes de ce journaul sont constituées de la date, l'heure, la classe et la méthode où s'est produit l'événement noté dans le journal, et un message.

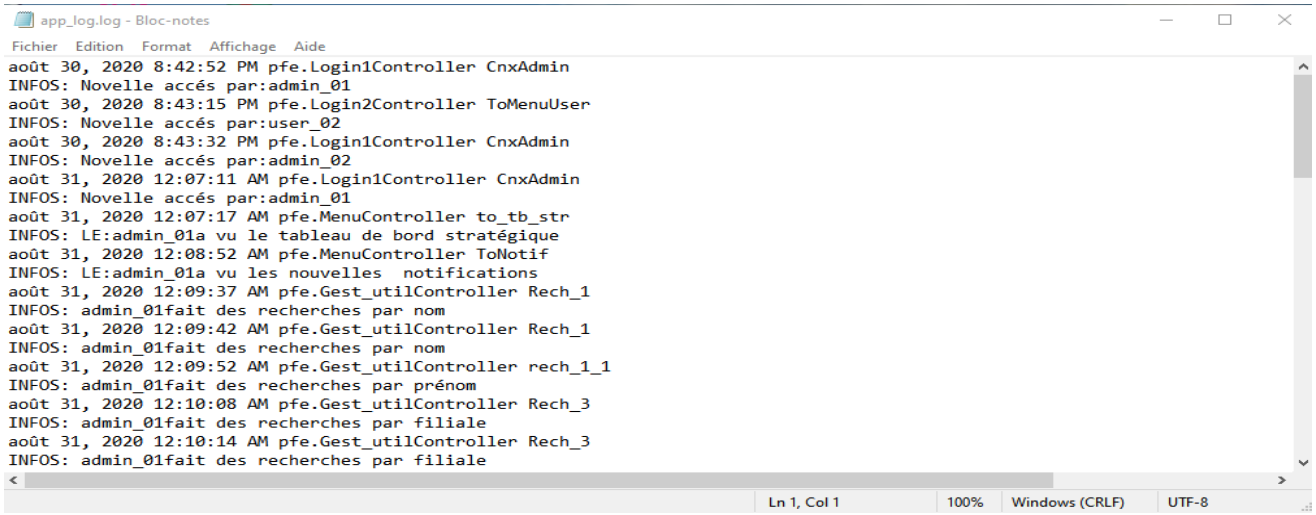


Figure V.2-2: Aperçus du fichier log de notre application

V.2.3.2) **AES (Advanced Encryption Standard) :**

Afin de protéger les informations particulièrement sensibles comme nos mots de passe nous avons utilisé l'AES aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Son fonctionnement s'explique comme suit :

L'algorithme prend en entrée un bloc de 128 bits (16 octets), la clé fait 128, 192 ou 256 bits. Les 16 octets en entrée sont permutés selon une table définie au préalable. Ces octets sont ensuite placés dans une matrice de 4x4 éléments et ses lignes subissent une rotation vers la droite. L'incrément pour la rotation varie selon le numéro de la ligne. Une transformation linéaire est ensuite appliquée sur la matrice, elle consiste en la multiplication binaire de chaque élément de la matrice avec des polynômes issus d'une matrice auxiliaire, cette multiplication est soumise à des règles spéciales selon GF(28) (groupe de Galois ou corps fini). La transformation linéaire garantit une meilleure diffusion (propagation des bits dans la structure) sur plusieurs tours.

Finalement, un OU exclusif XOR entre la matrice et une autre matrice permet d'obtenir une matrice intermédiaire. Ces différentes opérations sont répétées plusieurs fois et définissent un « tour ». Pour une clé de 128, 192 ou 256, AES nécessite respectivement 10, 12 ou 14 tours. **[48]**

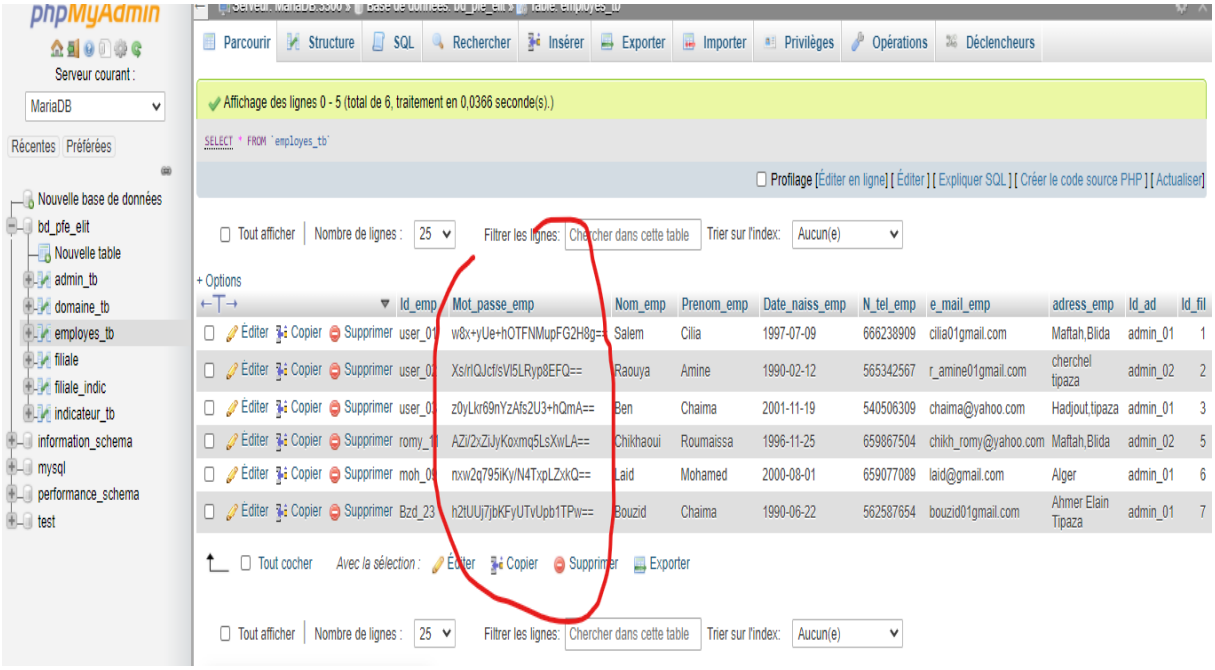


Figure V.2-3 : représentation des mots de passes cryptés dans notre base de données

V.3) Implémentation :

L'implémentation consiste à traduire le résultat obtenu lors de l'étape de conception en un programme ou logiciel informatique exécuté sur machine en utilisant les outils de programmation adaptés au problème à traiter, ainsi nous allons présenter le déroulement de notre application.

V.3.1) Présentation de l'application :

Après toute une étude approfondie et une conception adaptée nous somme arrivés à présenter l'application ci-dessus qui s'identifie en premier lieu par une interface d'accueil (figure) où il y a le choix d'accès entre deux sessions administrateur ou utilisateur.

Figure V.3-1: interface d'accueil

V.3.2) Session administrateur :

En entrant à la session administrateur, une interface de connexion s'affiche.

Figure V.3-2: interface de connexion

Après la connexion avec les bonnes conditions nous accédons à la page de l'administrateur.

Figure V.3-3: interface de l'administrateur

Nous allons expliquer un peux les différents boutons de l'interface de l'administrateur.

Donc l'administrateur peut voir son propre profil et modifier son mot de passe.

Figure V.3-4: interface du profil de l'administrateur

Comme nous savons déjà l'administrateur s'occupe de la gestion des utilisateurs, dans l'interface ci-dessus après avoir accéder à la gestion des utilisateur l'admin aura un aperçu général de tous les employés qu'il a ajouté, il peut rechercher un employé suivant différentes contraintes (nom, prénom,), il peut modifier leurs informations et mot de passe, ajouter un nouvel employé ou en supprimer un.

Figure V.3-5: interface de la gestion des utilisateurs

L'admin peut aussi ajouter un autre admin.

Figure V.3-6 : interface de l'ajout d'un admin

Dans l'interface des notifications on trouve deux parties, la partie des mises à jour qui va informer une semaine à l'avance que la date de la mise à jour de la valeur approche, et la partie notification qui nous informe sur les filiales qui ont dépasser leurs seuils de tolérance.

Figure V.3-7 : interface des notifications

L'administrateur et le seul responsable des indicateurs, il s'occupe de leur aperçus, leur ajout, leur contrôle, leurs modifications, suppression, leurs graphiques et fiches techniques.

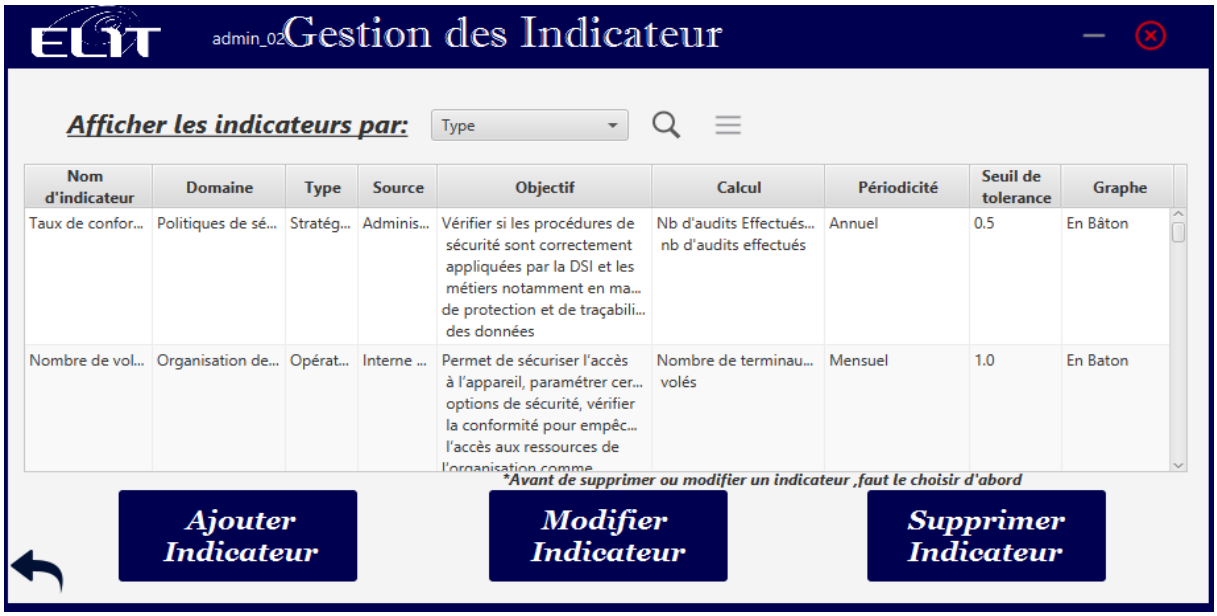


Figure V.3-8 : interface de la gestion des indicateurs

Nous précisons que lors de l'ajout d'un nouvel indicateur son graphique se génère automatiquement dans l'interface de son type.

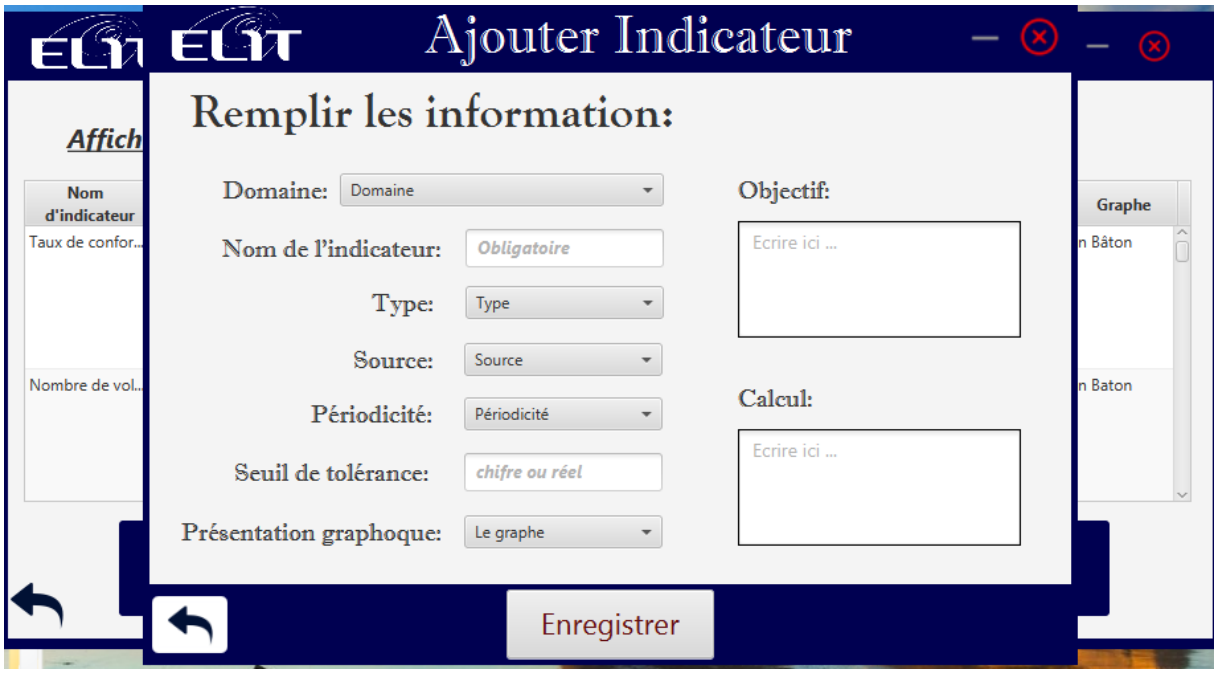


Figure V.3-9: interface de l'ajout d'un indicateur

En accédant à la partie tableau de bord stratégique l'administrateur aura un aperçu global des graphiques des indicateurs de types stratégiques, voir les variations des valeurs par rapport a la périodicité, remarquer les filiales qui ont dépassées leurs seuils de tolérance dans la barre des alertes.

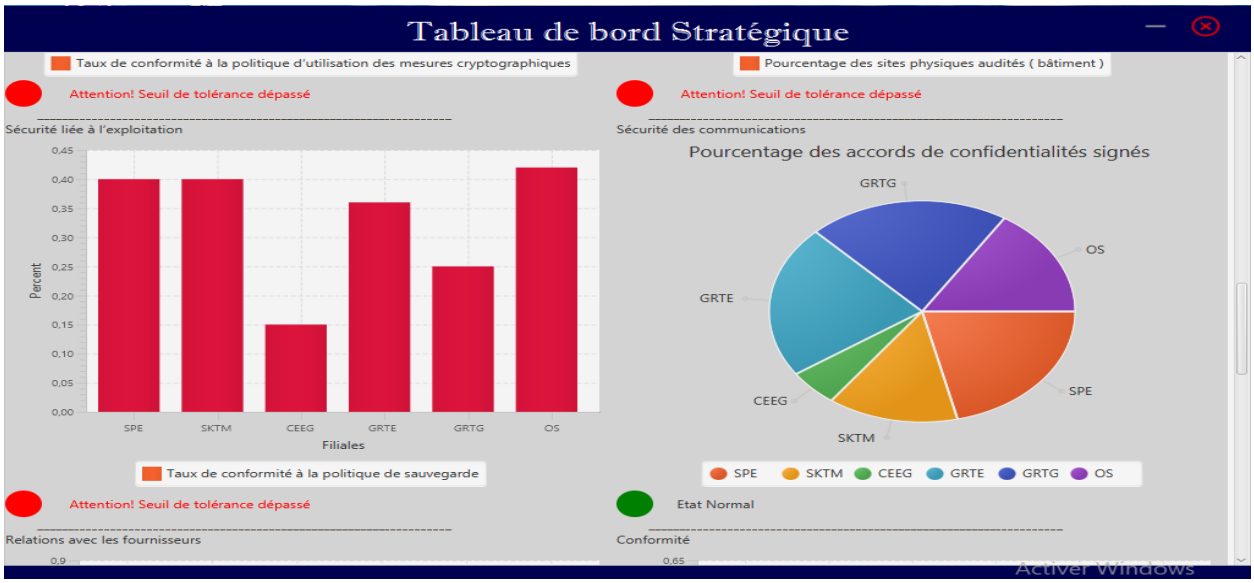


Figure V.3-10 : interface des tableaux de bord stratégiques

En accédant à la partie tableau de bord opérationnel l'administrateur aura un aperçu global des graphiques des indicateurs de types opérationnel, voir les variations des valeurs par rapport à la périodicité, remarquer les filiales qui ont dépassées leurs seuils de tolérance dans la barre des alertes, et comme tous les indicateurs opérationnels sont mensuels on pourra revoir les graphiques des mois précédents.

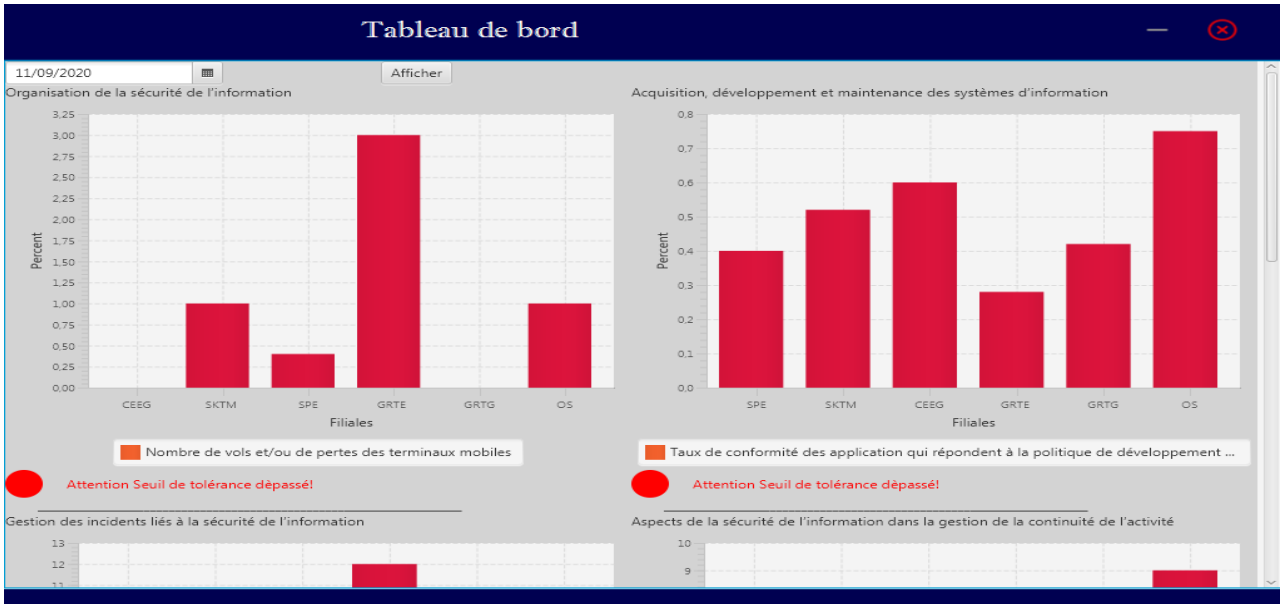


Figure V.3-11 : interface des tableaux de bord opérationnels

V.3.3) Session utilisateur :

En entrant à la session utilisateur (user), une interface de connexion s'affiche.

Figure V.3-12: interface de connexion de l'utilisateur

Après la connexion avec les bonnes conditions nous accédons à la page de l'utilisateur qui presque similaire à celle de l'utilisateur.

Figure V.3-13: interface de l'utilisateur

L'utilisateur peut seulement voir son profil et il n'a pas la permission de le modifier.

Figure V.3-14: interface de profil utilisateur

Il a la même de notifications que l'administrateur.

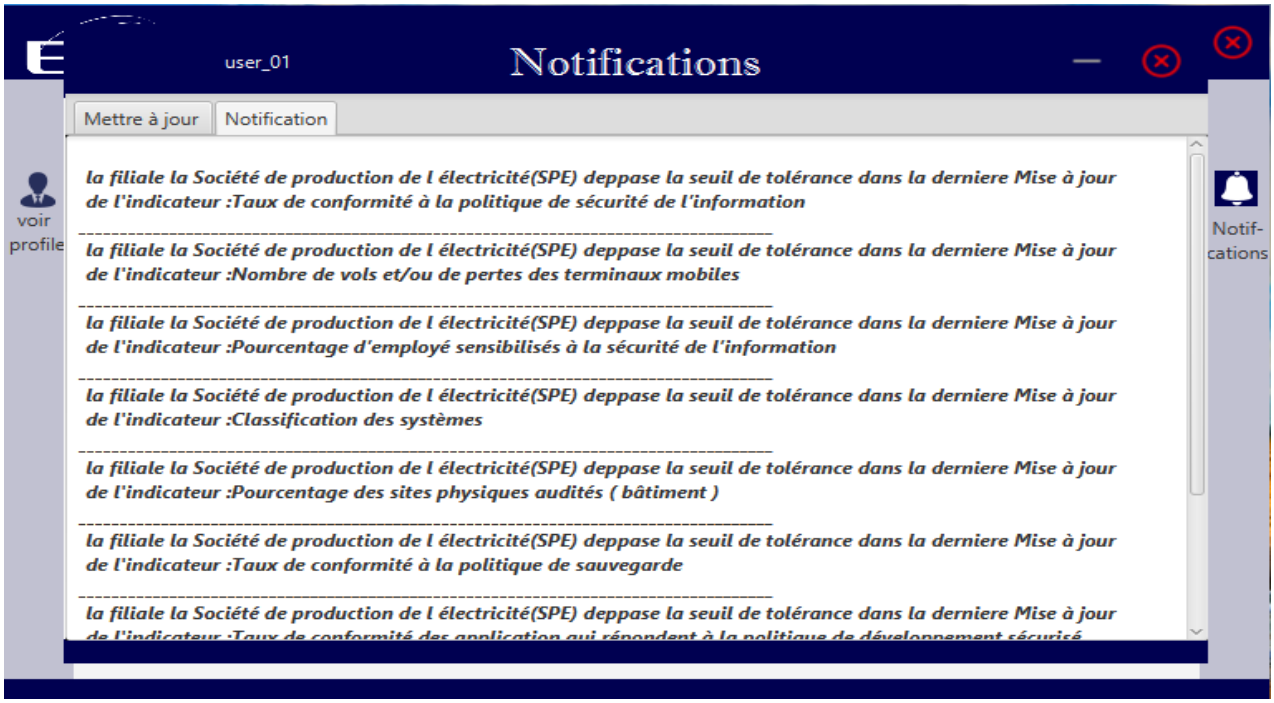


Figure V.3-15: interface des notifications de l'utilisateur

Concernant les indicateurs, l'utilisateur peut que voir les fiches techniques des indicateurs, en sélectionner un et ajouter la valeur de celui-ci après l'avoir calculé lorsque sa périodicité approche, et il n'a pas le droit de l'ajouter avant.

Figure V.3-16: interface de la liste des indicateurs

En accédant à l'interface des tableaux de bord stratégiques et opérationnels, l'utilisateur aura la même interface que celle de l'administrateur

V.4) Conclusion :

Dans ce chapitre, nous avons présenté l'application réalisée. Celle-ci a réussi à avoir un avantage de plus par rapport à d'autres outils similaires en réalisant le même but. De plus, elle représente une vraie convivialité d'utilisation du fait que nous pouvons contrôler la sécurité de notre entreprise en toute simplicité.

Conclusion générale

Nous sommes arrivés maintenant au terme de ce mémoire. Tout au long de notre travail qui consiste à créer et automatiser un tableau de bord sécurité, et après de larges recherches bibliographiques approfondis sur la sécurité, nous avons constaté que la plupart des entreprises des pays développés et ceux en voie de développement, tel est le cas de l'Algérie, se trouvent confrontées à des degrés plus ou moins variables, aux mêmes menaces de sécurité de leurs systèmes d'information.

Aujourd'hui, la stratégie et le choix des outils de pilotage, de la politique de sécurité de l'information et des systèmes informatiques rendent la gestion de la sécurité, une réelle problématique au sein de l'entreprise.

SONELGAZ, au même titre que les autres entreprises publiques algériennes se trouve aujourd'hui dans un contexte de développer une sécurité unique et imbattable, afin de conserver voire, accroître ses parts du marché et se développer sereinement.

Dans la perspective de garantir sa pérennité et demeurer leader, SONELGAZ a adopté une démarche de modernisation. Celle-ci est passer par l'élaboration d'une PSI qui a était transmis par la filiale ELIT afin de les aider à générer des indicateurs de sécurité et les organiser dans un tableau de bord pour faciliter la surveillance et le contrôle de la sécurité au sein de SONELGAZ.

On a donc enrichi nos connaissances afin d'implémenter le tableau de bord sécurité qui répond à tous les besoins proposés par ELIT.

Cette implémentation passe toutefois par la prise de connaissance des normes de l'ISO, l'étude de la PSI de SONELGAZ, l'élaboration et calcul des indicateurs de sécurité, et enfin les organiser dans un tableau de bord.

Perspectives :

Le premier but du travail a été atteint. Toutefois, notre tableau de bord est ouvert à de futurs travaux visant l'amélioration de celui-ci. En effet, nous pourrions par exemple l'élargir vers d'autre domaine plus ou moins complexes pas seulement les problèmes de sécurité.

LISTE BIBLIOGRAPHIQUE :

1. « La sécurité de l'information : un des enjeux majeurs du XXIème siècle » disponible sur : http://www.datacert27001.com/securite-informatique/la-securite-de-linformation-un-des-enjeux-majeurs-du-xxieme-siecle/
2. Rafika BOURAIB née BOUROKBA « Tableaux de Bord, Outils de Pilotage de Mesure et d'Evaluation de la Performance de l'Entreprise. Cas Pratique NAFTAL », 2014/2015.
3. Le bureau conseil de la DCSSI, « Guide pour l'élaboration d'une politique de sécurité de système d'information PSSI SECTION 1 : introduction », page 5.
4. Idem **[3]** page 8.
5. Livre : Collège Lionel-Groulx POLITIQUE DE SÉCURITÉ INFORMATIQUE,2017.
6. Livre intitulé Sécurité informatique 2°edition Principes et méthode à l'usage des DSI, RSSI et administrateurs par Laurent Bloch Christophe Wolfhugel, 15 mai 2013.
7. Idem **[3]** page 10.
8. Le bureau conseil de la DCSSI, « Guide pour l'élaboration d'une politique de sécurité de système d'information PSSI SECTION 2 : Méthodologie », 3 mars 2004, page 6.
9. Idem **[8]** page 8.
10. Idem **[8]** page 9.
11. Idem **[8]** page 6.
12. ISO/CEI 27002, 2013. « Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information », International Organisation for Standardisation, Genève.
13. « Présentation de la norme ISO 27002 – code de bonnes pratiques pour le management de la sécurité de l'information », 2016, disponible sur : https://www.infoqualite.fr/presentation-de-la-norme-iso-27002-code-de-bonnes-pratiques-pour-le-management-de-la-securite-de-linformation/
14. Idem **[13]**.
15. Pierre Voyer, Tableau de bord de gestion et indicateurs de performance, 2e édition, 1999, Presses de l'Université du Québec, Sainte-Foy, P. 61

16. CLUB DE LA SECURITE DES SYSTEMES D. INFORMATION FRANÇAIS, INDICATEURS DE SECURITE, Juillet 2001.

17. Fernandez Alain, 2005, l'essentiel du tableau de bord, Ed Groupe Eyrolles

18. Idem **[17]**

19. Pierre Voyer, Tableau de bord de gestion et indicateurs de performance, 2e édition, 1999, Presses de l'Université du Québec, Sainte-Foy, P. 65

20. Le contrôle de gestion au service de la performance de l'entreprise par El bachir Rouimi IBN ZOHR - la licence dans la gestion 2010

21. Malo, encyclopédie de gestion, ED Economica, Paris ,1997

22. Voyer, Pierre, Tableaux de bord de gestion et indicateurs de performance ed2, 2006, p54...55

23. Livre : « Le tableau de bord de la DSI : un outil pour mieux piloter son informatique. » , hery.ramananarivo@voirin-consultants.com, juin 2004.

24. Livre, Elaboration de tableaux de bord SSI, 5 février 2004 p5.

25. Idem **[23]**, p3.

26. Idem **[23]**, p9.

27. Ludovic Aubut-Lussier, Le tableau de bord: ABC et meilleures pratiques, février 2013, P 14.

28. Idem **[24],** p7.

29. Idem **[24],** p9…56.

30. www.iso.org.

31. CLUB DE LA SECURITE DES SYSTEMES D. INFORMATION FRANÇAIS, LES METRIQUES DANS LE CADRE DE LA SERIE 27000, mai 2019, p16.

32. Idem **[31],** p9.

33. Idem **[30].**

34. Idem **[31],** p11.

35. Idem **[31],** p14.

36. Sana SELLAMI « Conception et Réalisation d'un outil de génération automatique de Mappage pour la transformation de documents XML », 2005/2006.

37. David J. Eck, « Introduction to Programming Using Java ». Disponible sur : math.hws.edu/eck/cs124/downloads/javanotes6-linked.pdf.

38.« Présentation de JAVA», disponible sur : http://www.mcours.net/cours/pdf/info/presentation_de_java.pdf.

39.« Introduction à SQL: Qu'est-ce que SQL?» disponible sur : https://www.scriptol.fr/sql/sql-introduction.php.

40.« NetBeans - Définition et Explications» disponible sur : https://www.techno-science.net/definition/5346.html.

41.« NetBeans IDE» disponible sur : https://www.oracle.com/ch-fr/tools/technologies/netbeans-ide.html.

42.« Introduction à JavaFX» disponible sur : https://www.labri.fr/perso/johnen/pdf/IUT-Bordeaux/UMLCours/IntroductionJavaFX-V1.pdf.

43.« JavaFX aide à créer l'interface d'une application Java» disponible sur : https://www.scriptol.fr/programmation/javafx.php

44.« WAMPSERVER40 » disponible sur : https://www.memoireonline.com/10/17/10084/m_Conception-et-transformation-d-une-application-web-en-application-mobile12.html.

45.« phpMyAdmin » disponible sur : http://moodle.lyceestendhal.it/pluginfile.php/843/mod_label/intro/phpMyAdmin.pdf.

46.« MariaDB » disponible sur : https://sql.sh/sgbd/mariadb.

47. Tarek LABIDI: « Computer Forensics Investigation, Analyse des fichiers LOG » disponible :http://www.securinets.com/sites/default/files/fichiers_pdf/Analyse%20des%20fichiers%20LOG.pdf

48.https://fr.wikipedia.org/wiki/Advanced_Encryption_Standard.