République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Saad Dahleb Blida

Faculté des sciences

Département d'Informatique

Mémoire de fin d'études

Pour l'obtention du diplôme de Master en informatique

Option : Sécurité des systèmes d'informations

Thème :

Analyse et mise en œuvre d'un système de management de la sécurité de l'information (SMSI) au sein de l'entreprise UNIDEES

Réaliser par :

- AISSA Hasnaa
- BOUDISSA Abedelmoumene

Encadré par :

Mr OULDKHAOUA Mohamed

Mr BEDRANI Omar

Promotion : 2016/2017

Remerciement

*Avant toute chose, Nous remercierons **ALLAH** le tout puissant, de nous avoir donnée la force et la patience pour mener à terme ce travail.*

Nous présentons nos sincères remerciements à notre promoteur Mr OULEDKHAOUA Mohamed pour avoir assuré le suivi de ce projet mais aussi pour leur soutien, leurs conseils et leur disponibilité.

Nous tenons également à remercier, Mr BEDRANI Omar, responsable de la direction technique, Mr Emir et Mr Nadjib et Mr ZAKARIA Mahdi pour nous avoir acceptés et suivis tout au long de ce projet de fin d'études.

Nous tenons à remercier aussi tous nos enseignants qui ont participé à notre formation tout au long de notre cursus.

Nous tenons à remercier nos parents, nos familles et amis pour leur soutien tout au long de ce mémoire.

Nous remercions également toutes ces personnes sur internet qui ont partagé leurs connaissances et expériences et répondu à nos questions, ils nous ont été d'une grande aide.

Enfin, nous remercions tous ceux qui ont aidé de près ou de loin à l'élaboration de ce mémoire et à la réussite de ce projet.

Table des matières

Liste des figures :

Liste des tableaux :

Résumé :

Le présent rapport expose le travail que nous avons réalisé dans le cadre du projet de fin d'études effectué au sein de l'entreprise UNIDEES (Algérie), ayant comme objectifs l'analyse et la mise en œuvre d'un SMSI conforme aux exigences de la norme ISO/CEI 27001.

On faisait appel, à une certaine étape avant la mise en œuvre de la mission de SMSI et à l'analyse des risques d'où la nécessité d'élaborer une étude sur les normes et référentiels en matière de sécurité de l'information suivi par une étude comparative entre les méthodologies les plus utilisées dans la gestion des risques (EBIOS et MEHARI).

La mission essentielle dans notre projet qui est la mise en œuvre d'un SMSI s'est déroulée en 4 phases principales. Tout d'abord, on a fait une étude détaillée sur l'entreprise pour bien comprendre les processus métier, les outils de sécurité existants et leur fonctionnement et en fin les objectifs de l'entreprise en matière de sécurité de l'information, après on a présenté la série des normes ISO 27000, en suite on a expliqué les étapes d'implémentation de cette dernière et en fin on a fait des recommandations pour que l'entreprise puisse être conforme aux exigences d'ISO 27001.

Les mots clés :

ISO/IEC 2700x, SMSI, EBIOS, MEHARI, Top 10OWASP.

ملخص:

هذا التقرير يعرض العمل الذي قمنا به في إطار مشروع التخرج، التي اجريت على مستوى شركة (UNIDEESالجزائر)، والهدف منه تحليل وتنفيذ نظام إدارة أمن المعلومات SMSI وفقا لمتطلبات المعيار ISO 27001 .

بالإضافة إلى ذلك، في مرحلة معينة قبل تنفيذ المهمة قمنا بتحليل المخاطر ومنه الحاجة إلى إعداد دراسة عن معايير سلامة معلوماتية تليها دراسة مقارنة بين المعايير الأكثر استخداما في منهجيات إدارة المخاطر (EBIOS وMEHARI).

والمهمة الأساسية لمشروعنا هي تنفيذ نظام إدارة أمن المعلومات في أربع مراحل رئيسية. أولا، تقديم دراسة مفصلة عن العمل لفهم العمليات المهنية، وأدوات الأمن الحالية وتشغيلها وأخيرا أهداف الشركة الحالية في خصوص أمن المعلومات، بعدها نقدم دراسة مفصلة حول سلسلة ISO 27000، ثم شرحنا خطوات تطبيقها، وفي النهاية قدمنا توصيات للشركة تتوافق مع متطلبات ISO 27001 حتى تكون مطابقة للمعايير الدولية.

الكلمات المفتاحية

ISO/IEC 2700x, SMSI, EBIOS, MEHARI, Top 10OWASP.

Abstract:

This report sets out the work we have carried out as part of the final project carried out at UNIDEES (Algeria), with the objectives of analyzing and implementing an ISMS that complies with the requirements Of ISO / CEI 27001 standard.

In addition, at some stage prior to the implementation of the ISMS mission and the risk analysis, a study on standards and safety standards was called for, Information followed by a comparative study between the most used methodologies in risk management (EBIOS and MEHARI).

The essential mission in our project is the implementation of ISMS took place in four main phases. First, a detailed study of the company was carried out in order to understand the business processes, the existing security tools and their functioning and, finally, the company's information security objectives. After presented the ISO 27000 series of standards followed by an explanation of the implementation stages of the ISO 27000 standard and, finally, the recommendations were made for the company to comply with the requirements of ISO 27001.

Keywords:

ISO/IEC 2700x, SMSI, EBIOS, MEHARI, Top 10OWASP.

Introduction générale :

Contexte :

L'information, sa gestion et sa sécurité sont aujourd'hui plus que jamais des enjeux de management à part entière. Comme l'exprime Jérôme Denis « L'informatique et sa sécurité impliquent un paradoxe qui consiste en un développement sans précédent de l'efficacité mais aussi de la fragilité technique des organisations. Les technologies de communication et systèmes d'information sont à la fois l'occasion de démultiplier la circulation d'informations dans une entreprise comme source d'avantage concurrentiel mais elles peuvent aussi la rendre vulnérable à certaines menaces. Les pratiques de management doivent désormais évoluer pour intégrer au niveau de la gouvernance même de l'entreprise la préoccupation d'une sécurisation de l'information de l'entreprise qui constitue un actif (immatériel) à part entière ». Ces dernières sont un enjeu de management car elles impliquent des risques et un régime de fragilité permanente pour l'entreprise, pouvant impacter la qualité des biens et services fournis (notamment dans la fiabilité des informations fournies). Dans un monde interconnecté, l'information, les processus, les systèmes et les réseaux qui s'y rapportent constituent des actifs critiques de l'organisation. Les organisations et leurs systèmes et réseaux d'informations sont confrontés à des menaces pour la sécurité ayant de multiples sources, notamment la fraude assistée par ordinateur, l'espionnage, le sabotage, le vandalisme, les incendies et les inondations. Les dommages causés aux systèmes et aux réseaux d'information par des programmes malveillants, le piratage informatique et les attaques par saturation deviennent plus courants, plus ambitieux et de plus en plus sophistiqués.

Face à cela, la norme ISO 27001-2013 a comme objectif de répondre à cet enjeu de management en envisageant la sécurité de l'information comme un projet transverse.

La norme ISO 27001 est, à la base, issue de la série des normes ISO 27000. Cette norme décrit les exigences nécessaires à la mise en œuvre du système de management de la sécurité de l'information (SMSI).

L'implémentation d'un SMSI est la garantie de l'adoption de bonnes pratiques, de l'augmentation de la fiabilité et la certification par un organisme indépendant assurera l'apport de la confiance des parties prenantes de l'entreprise (clients, fournisseurs, actionnaires, banques, autorités…).

Ce rapport présent l'implémentation d'un SMSI au sein de l'entreprise UNIDEES Algérie.

Problématique :

L'information est aujourd'hui la sève des entreprises. C'est ce qui fait à la fois sa force et son existence. Fichiers, bases de données, méthodes de travail et de fabrication, fiches des salariés et informations industrielles sont autant d'informations qui composent la structure et la base d'une entreprise. Il s'agit là de son capital intellectuel, ou plutôt capital informationnel. Toute perte d'information peut porter un coup fatal à une entreprise.

Si ces informations venaient à être perdues, volées ou à tomber dans les mains d'une autre entreprise, la donnée n'aurait plus de raison d'exister car elle ne serait plus exclusive. L'information a aujourd'hui de la valeur de par son côté unique et exclusif pour une entreprise. Il est donc dans l'intérêt de l'entreprise de protéger son patrimoine informationnel.

Objectifs :

Notre projet consiste à repérer et définir les informations critiques pour l'entreprise 'UNIDEES', choisir les mesures de sécurité adéquates, et contrôler leur mise en œuvre.

La sécurité de l'information c'est 80% d'organisation et 20% de technologie, il faut savoir comprendre et gérer les risques spécifiques, organiser un projet sécurité, s'appuyer sur des normes et des méthodes, et identifier les coûts et les gains.

Et pour cela on s'est basé sur l'aspect organisationnel en utilisant la série des normes ISO/IEC 2700X qui traduisent bien l'importance des aspects organisationnels et managériaux.

Les attaques de toutes natures se développent et se complexifient. Les attaques les plus fréquentes sont les attaques externes de type "hacker", car elles sont automatisables, réalisables à distance et donnent à l'attaquant un sentiment d'impunité. En effet les attaques venant de l'interne représente un grand danger pour les entreprises ou organismes (vol d'informations critiques, détournement de fonds, dénigrement d'image de l'entreprise, ...).

La sécurité a donc une dimension humaine majeure et un caractère collectif : "la sécurité de mes informations dépend du comportement de mes voisins et vice versa", c'est donc, dans les entreprises une question de management, et c'est pour cela que notre application va se basé sur l'aspect humain et sa sensibilisation et créer un moyen de communication entre le responsable de sécurités et le reste du personnels au niveau de l'entreprise.

Contenu du mémoire :

Pour présenter au mieux notre travail, nous avons structuré ce document en trois chapitres. Avant d'entamer ces trois chapitres nous avons introduit le contexte de notre étude et fixé la problématique ainsi que les objectifs du projet.

Le contenu des trois chapitres peut être résumé comme suit :

Chapitre 1 Etat de l'art : Ce chapitre est composé de deux parties, la première consiste à présenter les notions théoriques relatives de notre projet et la deuxième partie consiste à présenter l'organisme d'accueil et les solutions de sécurités existantes.

Chapitre 2 : La série des normes ISO/IEC 27000, Nous abordons l'étude détaillée des normes de la série ISO/IEC 2700x.

Chapitre 3 : Analyse et Implémentation de SMSI et présentation de la solution UNICOM, ce chapitre est composé de deux parties, dans la première partie nous présentons les différentes étapes de la méthode EBIOS, et la deuxième partie nous procédons à la réalisation et au déploiement de la solution conçue. Nous débutons avec la présentation de l'environnement de déploiement puis on décrivant l'utilité de l'application proposé.

Nous clôturons notre document avec une conclusion générale où nous synthétisons notre travail.

Liste des abréviations :

ACL Acces Control Liste

AFAI Association Française de l'Audit et du Conseil Informatique

ANSSI L'Agence Nationale de la Sécurité des Systèmes d'Information.

AP Acces Point

CAN Canaux interpersonnels.

CSS Cascading Style Sheets.

EBIOS Expression des Besoins et Identification des Objectifs de Sécurité.

HTML HyperText Markup Language.

IEC Commission électrotechnique internationale.

ISACA Information Systems Audit and Control Association

ISO Organisation internationale de normalisation.

ITIL référentiel de bonnes pratiques en matière de gestion du système d'information

JTC le Joint Technical Committee

LOC Locaux du l'entreprise.

LOG logiciel.

MAT matériel.

MEHARI Méthode Harmonisée d'Analyse des Risques.

ORG Organisation du l'entreprise.

OWASP Open Web Application Security Projet

PAP Supports papier.

PCI DSS Payment Card Industry Data Security Standard.

PDCA processus de gestion de continuité (Plan, Do, Check, Act)

PER Personnes.

PHP Hypertext Preprocessor.

RACI matrice(**R** : responsable, **A** : acteur, **C** : consulté, **I** : informé).

SMSI Système de Management de Sécurité de l'Information.

SQL Structured Query Language.

SYS système.

TI Technologies de l'Information

WAB Wallix Admin Bastion

WAF firewall application Web

XSS script cross-site

Chapitre 1 :

Etat de l'art

Ce chapitre est composé de deux parties, la première consiste à définir les notions et les termes relatifs à notre projet, la deuxième partie consiste à présenter l'organisme d'accueil (UNIDEES Algérie) et cartographier leurs outils de sécurité existants.

Partie 1 : Vue globale et vocabulaire :

L'objectif de cette première partie est de définir les défirent termes qu'on va les utiliser dans le reste du projet.

1. Termes et définitions générale :

1. Systèmes :

Un système est un ensemble d'éléments en relation les uns les autres et formant un tout. Il représente une unité parfaitement identifiable et évoluant dans un environnement. Il existe donc une limite qui départage le système de son environnement.

2. L'information :

Est un actif qui, comme tous les autres actifs importants de l'organisme, est essentiel à son fonctionnement et qui, par conséquent, requiert une protection adéquate. Elle peut être stockée sous différentes formes, notamment numérique (par exemple : un support électronique ou optique), matériel (par exemple : papier) ou en tant qu'information intangible (par exemple : connaissance du salaire). Elle peut être transmise par différents moyens. [9]

3. Sécurité de l'information

La sécurité de l'information garantit la confidentialité, la disponibilité et l'intégrité de l'information. Afin de contribuer au succès de l'organisme et à sa pérennité, et de réduire le plus possible l'impact des incidents liés à la sécurité de l'information, elle implique l'application et le management de mesure de sécurité appropriées, ce qui sous-entend la prise en compte d'un vaste éventail de menaces.[1]

- La disponibilité : garantir l'accès à l'information en tout temps.
- L'intégrité : Garantir que l'information est bien celle que l'on croit être.
- La confidentialité : assurer que seules les personnes autorisées aient accès à l'information.

4. Système d'Information :

Un système d'Information (noté SI) est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui représente l'ensemble des éléments

participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'entreprise. A l'origine les systèmes d'informations ont fait leur première apparition dans les domaines de l'informatique et des télécommunications, cependant nous voyons aujourd'hui apparaître le concept dans tous les secteurs, que ce soit des entreprises privées ou publiques.

Un système d'information peut être apparenté au véhicule qui permettra d'établir la communication dans toute l'entreprise. La Structure du système est constituée de l'ensemble des ressources (hommes, matériels, logiciels) qui s'organise pour : collecter, stocker, traiter et communiquer les informations. Le système d'information est le grand coordinateur des activités de l'entreprise et qui joue un rôle crucial dans l'atteinte des objectifs fixer par cette dernière. Le SI se construit tout autour des processus « métier » et ses interactions. Pas seulement autour des bases de données ou des logiciels informatiques qui le constitue. Le SI doit être en accord avec la stratégie de l'entreprise.

2. Les termes qui sont définie dans la norme 27000 :

La présente Norme internationale offre une vue d'ensemble des systèmes de management de la sécurité de l'information et définit les termes qui s'y rapportent.

Terme	Définition
Contrôle d'accès	Moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les exigences propre à la sécurité et à l'activité métier.
Attaque	Tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un actif, ou de faire un usage non autoriser à celui-ci.
Audit	Processus méthodique, indépendant et documenté permet d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits.
Mesure	Processus permet de déterminer une valeur.
Non-conformité	Non-satisfaction d'une exigence.
politique	Intention et orientation d'un organisme telles que formaliser par sa direction.
Exigence	Besoin ou attente formulé, généralement implicite ou obligatoire.
Risque	Effet de l'incertitude sur l'atteinte des objectifs.
Risque résiduelle	Risque subsistant après le traitement du risque.
Actif (asset)	C'est toute chose tangible ou intangible ou caractéristique qui

	a de la valeur à une organisation. Il existe de nombreux types d'actif. Certains incluent des choses évidentes comme les machines, les installations, les brevets et les logiciels. Mais le terme peut également inclure des choses moins évidentes telles que les services, l'information et les gens, et des caractéristiques telles que la réputation et l'image ou des compétences et des connaissances. [10]

Tableau 1 Termes relative à la série des normes ISO/IEC 27000

Partie 2 : Présentation de l'entreprise d'accueil :

UNIDEES Algérie, entreprise spécialisée dans le conseil, l'intégration et l'infogérance en sécurité des systèmes d'information, évolue dans des environnements où l'exigence est permanente (Energie, Industries, Défense, Télécom…). Ses missions de conseil ainsi que son expérience des projets d'intégration et d'infogérance menés dans des environnements complexes, sensibles et critiques, lui permettent d'accompagner durablement ses clients dans leur activité, en répondant à leurs exigences de transformation.

La pérennité et la sûreté des systèmes font notamment partie des préoccupations essentielles d'UNIDEES Algérie, qui place la sécurité au cœur de chacun de ses projets. A cette culture de la rigueur s'ajoutent la détermination à prendre des engagements forts en termes de résultats et la conviction que la réussite se fond sur la qualité des hommes, leurs compétences et leur éthique.

Chaque jour, les collaborateurs d'UNIDEES Algérie contribuent au développement et à la performance des entreprises.

Leurs clients ont des métiers différents, mais ils partagent un même besoin, de fiabilité, de qualité, de rigueur, d'innovation et de sécurité quand il s'agit de gérer leurs systèmes sensibles. [1]

Figure 1 Partenaire et expertise [1]

1. Les déférentes directions d'UNIDEES :

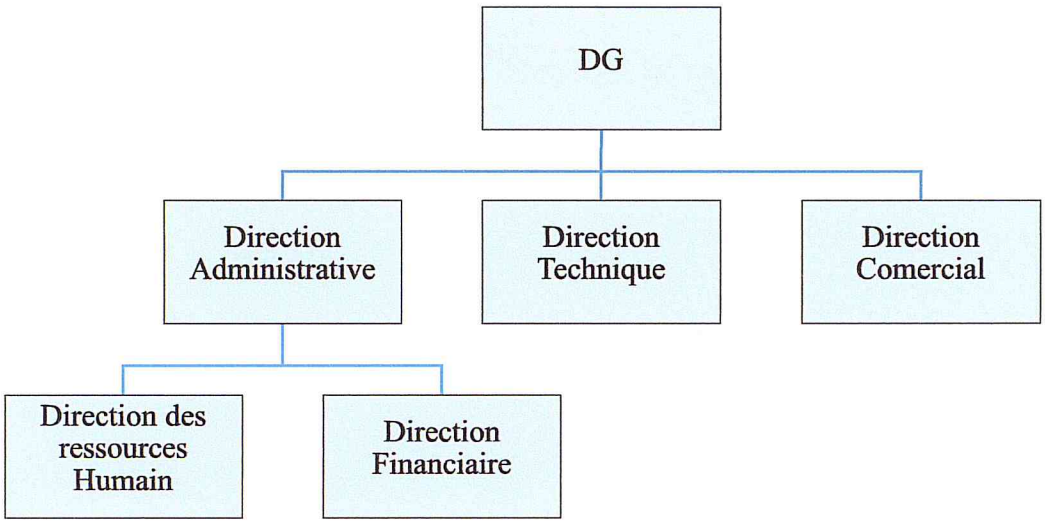


Figure 2 Organigramme d'UNIDEES

2. L'architecture générale du réseau chez UNIDEES :

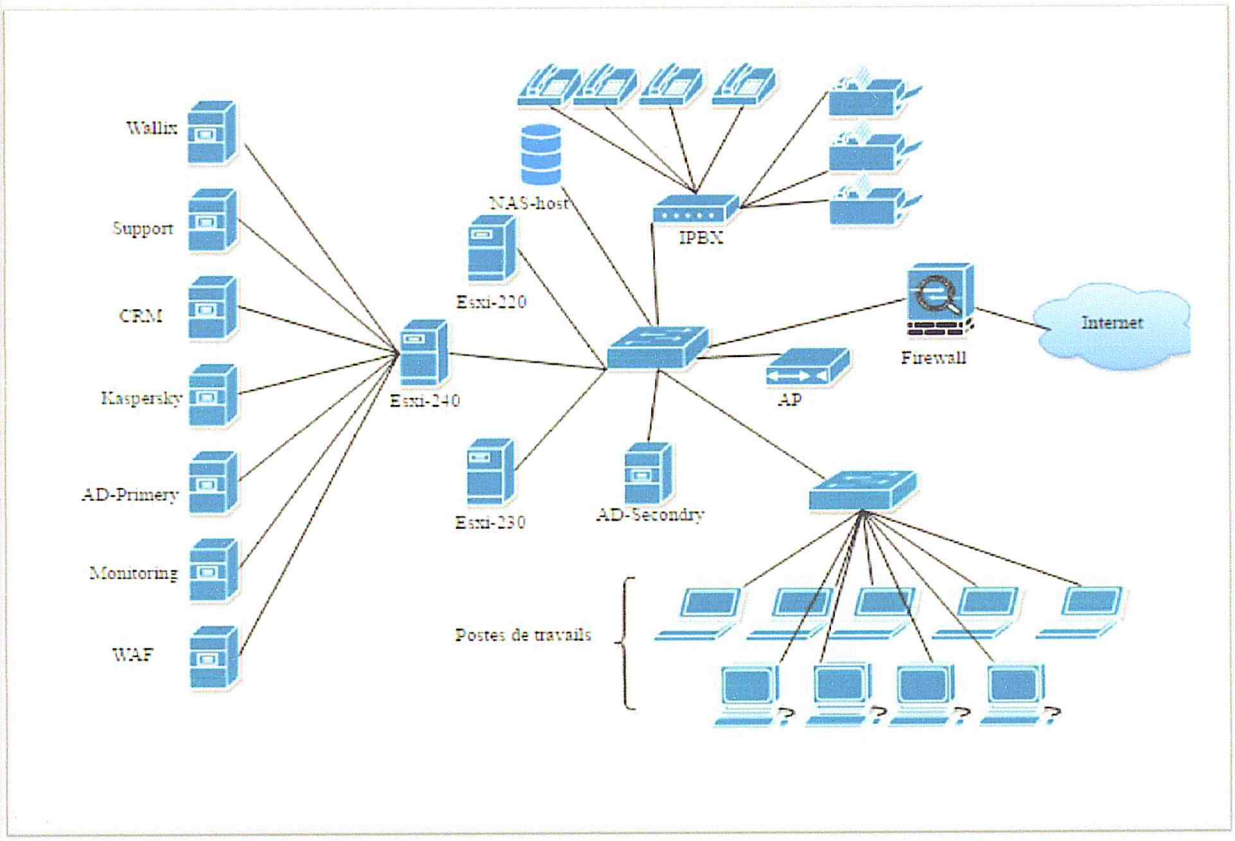


Figure 3 Architecture du réseau d'UNIDEES

- **Description de chaque actif de l'architecture du réseau :**

Actif	Description
Esxi-220	Serveur des tests.
Esxi-230	Serveur des workshops.
Esxi-240	Serveur principale de UNIDEES, il contient tous les informations essentiel relative à l'entreprise et ces clients, il est devisé en sous serveur (des hyper viseur) virtuellement.
Firewall	Contient tous les ACL interne et externe.
Wallix	Outil de traçabilité des utilisateurs à privilège.
Support	Application de communication entre l'entreprise et ces clients.
CRM	Application qui gère les informations des clients et fournisseurs (adresse, facture...).
Serveur Kaspersky	Serveur de l'antivirus Kaspersky.

Serveur AD-Secondry	Les Active-directory secondaire (une copie de réserve).
Serveur Monitoring	L'application de monitoring.
Serveur AD-Primery	Les Active-directory principal.
NAS-Host	Une pile des disques, pour le stockage des données.
IPBX	Distributeur des lignes téléphoniques et fax.
AP	Point d'accès WIFI.

Tableau 2 déscription des actifs de réseau d'UNIDEES

I. Les solutions de sécurité existantes chez UNIDEES

1. Le Pare-feu (matériel) :

Un pare-feu (ou *firewall*) est un outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

Un pare-feu matériel est destiné aux utilisateurs très exigeants, de grands réseaux ou des serveurs, il est souvent un dispositif autonome pour des particuliers ou des petites entreprises, celui-ci est d'habitude intégré dans un router/modem. Lorsqu'un pare-feu matériel est utilisé, tout trafic par réseau passe à travers celui-ci avant d'atteindre des ordinateurs individuels.

Lors du passage des données, le pare-feu matériel analyse le contenu en profondeur afin de décider si elles peuvent passer ou non. Il y a des pare-feu ne faisant rien d'autre que de suivre des règles établies par l'utilisateur.

Par exemple : Ne laisser personne établir une connexion depuis Internet vers un ordinateur local se trouvant derrière le pare-feu, n'autoriser que les connexions sortantes.

D'autres pare-feu appliquent des règles plus avancées en s'appuyant sur des filtres de protocoles. Par exemple : Laisser des utilisateurs se connecter à Internet, mais seulement via le port 80 (le port destinés aux serveurs web HTTP) et faire passer le trafic entrant vers un serveur web situé derrière le pare-feu avant d'atteindre des ordinateurs individuels. Il y en a encore d'autres qui sont encore plus raffinés et analysent tout un paquet de données en profondeur en s'appuyant sur une couche application. Une telle règle pourrait être comme suit : Autoriser le trafic entrant via le port 80, à moins qu'il ne comprenne toute séquence de

code dont on peut se servir pour pirater le serveur web situé derrière le pare-feu, telle que des attaques par cross-site Scripting contre une base de données sur laquelle s'appuie le serveur web.

- **L'avantage d'un pare-feu matériel :**

Tout trafic doit passer par le pare-feu ou il n'atteindra pas d'ordinateur cible local. D'ailleurs, il n'y a pas de « surface d'attaque » supplémentaire au sein d'un pare-feu matériel permettant à un paquet de données malveillant de se glisser au travers du code manipulé, comme il serait possible avec un pare-feu logiciel. Les données passent ou non. Un bloc rectangulaire ne rentre simplement pas dans un trou rond.

- **L'inconvénient d'un pare-feu matériel :**

Un pare-feu matériel ne sait pas vraiment ce qui se passe sur les ordinateurs se trouvant derrière lui. Le pare-feu matériel ne voit que le trafic de données généré par ces ordinateurs, mais ne sait pas quelle application le génère.

Pour cela, si un utilisateur ordonne une application légitime de se connecter à Internet et que cette application essaie de se connecter d'une manière que le pare-feu matériel a été programmé à bloquer, ce dernier empêchera l'application de se connecter. De mauvaises décisions dues à des jeux de règles trop strictes bloquant des services légitimes sont un problème inhérent de pare-feu matériel et irritent en général les utilisateurs. [2]

- **La table suivante montre les différentes responsabilités sur le Pare-feu :**

Matrice RACI :

L'acronyme RACI, dans le management, représente une matrice des responsabilités : elle indique les rôles et les responsabilités des intervenants au sein de chaque processus et activité. Cette matrice représente l'organisation du travail en reliant dans un tableau commun la Structure de découpage de projet et la Structure organisationnelle du projet.

Les lignes de la matrice référencent les activités identifiées, et les colonnes les rôles (personnels impliqués par métier). Dans chaque cellule [activité ; rôle] figure la lettre « R », « A », « C » ou « I », où l'acronyme anglais RACI signifie :

R : responsible.

A : accountable (on utilise aussi parfois le terme approver).

C : consulted.

I : informed.

Type d'employée / Taches	IT Manager	Ingénieur de sécurité	Analyste des systèmes d'informations
Administration	I	R	C
Rapports de consultation	A	R	R
Déploiement	I	R	I
Tests	I	R	R

Tableau 3 Matrice RACI (Pare-feu)

2. L'antivirus Kaspersky Endpoint Security 10 :

- **Les composants de protection des postes de travail :**

- Antivirus Fichiers,
- Antivirus Courrier,
- Antivirus Internet,
- Antivirus IM,
- Pare-feu,
- Protection contre-attaques réseau,
- Surveillance du système,
- Contrôle du lancement des applications,
- Contrôle de l'activité des applications,
- Surveillance des vulnérabilités,
- Contrôle des périphériques,
- Contrôle Internet,
- Chiffrement des disques durs,
- Chiffrement des fichiers,
- Tâches d'analyse, de mise à jour et de recherche de vulnérabilités,

- Module externe de l'Agent d'administration Kaspersky Security Center 10.

  - **Les composants de protection des serveurs :**

- Antivirus Fichiers,
- Pare-feu,
- Protection contre-attaques réseau,
- Tâches d'analyse, de mise à jour et de recherche de vulnérabilités,
- Connecteur à l'Agent d'administration Kaspersky Security Center 10. [3]

  - **La table suivante montre les différentes responsabilités sur Kaspersky Endpoint Security 10 :**

Type d'employée / Taches	IT Manager	Ingénieur de sécurité	Analyste des systèmes d'informations
Administration	I	R	C
Rapports de consultation	A	R	A
Déploiement	I	R	C
Tests	I	R	R

Tableau 4 Matrice RACI (Kaspersky Endpoint security10)

3. Les pare-feu applicatifs web (WAF) :

Un firewall d'application Web (WAF) est un pare-feu d'application pour les applications HTTP. Il applique un ensemble de règles à une conversation HTTP. Généralement, ces règles couvrent les attaques courantes telles que le script cross-site (XSS) et l'injection SQL (TOP 10 OWASP).

Bien que les proxys protègent généralement les clients, les WAF protègent les serveurs. Un WAF est déployé pour protéger une application Web spécifique ou un ensemble d'applications Web. Un WAF peut être considéré comme un proxy inverse .

Les WAF peuvent se présenter sous la forme d'un appareil, d'un plugin de serveur ou d'un filtre, et peuvent être personnalisés dans une application. L'effort pour effectuer cette personnalisation peut être significatif et doit être maintenu pendant la modification de l'application.

Proxy : Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges. [4]

- **TOP 10 OWASP :**

Le Firewall d'application Web protège contre les risques de sécurité des applications Web les plus critiques, tels que l'injection SQL, les scripts inter-sites, l'accès illégal aux ressources, l'inclusion de fichiers distants et d'autres menaces de Top 10 OWASP.

La liste 2017 Top 10 OWASP a récemment été publiée pour commentaires du public. Elle est basée sur l'examen de plus de 2.3M vulnérabilités qui ont eu une incidence sur 50 000 applications et contient deux mises à jour de vulnérabilité à grande échelle et des scénarios d'attaque mis à jour. Examinons de plus près la liste dans son ensemble et quels changements clés ont été apportés dans les 10 principaux risques de sécurité des applications OWASP 2017. [5]

Rang	Top 10 OWASP	Description	La prévention
A1	Injection	Les défauts d'injection, tels que l'injection SQL, OS, XXE et LDAP, se produisent lorsque des données non fiables sont envoyées à un interprète dans le cadre d'une commande ou d'une requête. Les données hostiles de l'attaquant peuvent inciter l'interprète à exécuter des commandes involontaires ou à accéder à des données sans autorisation appropriée.	La séparation des données non fiables des commandes et des requêtes. L'option préférée consiste à utiliser une API sécurisée La validation d'entrée positive ou "liste blanche"
A2	Authentification cassée et gestion des sessions	Les fonctions d'application liées à l'authentification et à la gestion des sessions sont souvent implémentées de manière incorrecte, ce qui permet aux attaquants de compromettre les mots de	Un seul ensemble de contrôles d'authentification et de gestion de session forts Des efforts forts devraient également être faits pour éviter les défauts XSS qui peuvent être utilisés pour voler les identifiants de session.

		passe, les clés ou les jetons de session ou d'exploiter d'autres défauts de mise en œuvre pour assumer les identités des autres utilisateurs (temporairement ou définitivement).	
A3	Cross-Site Scripting (XSS)	Les défauts XSS se produisent chaque fois qu'une application comprend des données non fiables dans une nouvelle page Web sans validation ou échappement, ou met à jour une page Web existante avec des données fournies par l'utilisateur à l'aide d'une API de navigateur qui peut créer JavaScript. XSS permet aux attaquants d'exécuter des scripts dans le navigateur de la victime qui peuvent détourner les sessions des utilisateurs, défiler les sites Web ou rediriger l'utilisateur vers les sites malveillants.	échapper correctement aux données non fiables en fonction du contexte HTML (corps, attribut, JavaScript, CSS ou URL) dans lequel les données seront placées
A4	Contrôle d'accès brisé	Les restrictions sur ce que les utilisateurs authentifiés sont autorisés à faire ne sont pas correctement appliquées. Les attaquants peuvent exploiter ces défauts pour accéder à des fonctionnalités et / ou des données non autorisées, telles que accéder aux comptes d'autres utilisateurs, afficher les fichiers sensibles, modifier les données d'autres utilisateurs, modifier les droits d'accès, etc.	Un seul ensemble de contrôles d'authentification et de gestion de session forts Vérifiez l'accès Utiliser les références d'objets indirects par utilisateur ou session
A5	Confusion de sécurité (Security Misconfiguration)	Une bonne sécurité nécessite d'avoir une configuration sécurisée définie et déployée pour l'application, les cadres, le serveur d'applications, le serveur Web, le serveur de	Un processus pour se tenir au courant et déployer toutes les nouvelles mises à jour et correctifs Un processus automatisé pour vérifier que les configurations et

		base de données, la plate-forme, etc. Les paramètres sécurisés doivent être définis, mis en œuvre et maintenus, les défauts de sécurité étant souvent incurables. De plus, les logiciels doivent être mis à jour.	les paramètres sont correctement configurés
A6	Exposition de données sensibles	De nombreuses applications Web et API ne protègent pas correctement les données sensibles, telles que les finances, les soins de santé et les PII. Les attaquants peuvent voler ou modifier de telles données faiblement protégées pour effectuer une fraude par carte de crédit, un vol d'identité ou d'autres crimes. Les données sensibles méritent une protection supplémentaire, comme le cryptage au repos ou en transit, ainsi que des précautions particulières lors de l'échange avec le navigateur.	Assurez-vous de crypter toutes les données sensibles au repos et en transit. Ne stockez pas les données sensibles inutilement. Assurez-vous que les mots de passe sont stockés avec un algorithme spécialement conçu pour la protection par mot de passe, comme bcrypt, PBKDF2 ou scrypt .
A7	Protection contre l'attaque insuffisante	La majorité des applications et des API ne possèdent pas la capacité de base à détecter, prévenir et répondre aux attaques manuelles et automatisées. La protection contre les attaques va bien au-delà de la validation d'entrée de base et implique la détection, l'enregistrement, la réponse et même le blocage des tentatives d'exploitation. Les propriétaires d'applications doivent également être en mesure de déployer des correctifs rapidement pour protéger contre les attaques.	Détecter les attaques. Répondre aux attaques. Patch rapide.

A8	Cross-Site Request Forgery (CSRF)	Une attaque CSRF oblige le navigateur d'une victime connectée à envoyer une demande HTTP forgée, y compris le cookie de session de la victime et toute autre information d'authentification intégrée automatiquement, à une application Web vulnérable. Une telle attaque permet à l'attaquant de forcer le navigateur d'une victime à générer des demandes que l'application vulnérable pense être des demandes légitimes de la victime.	L'option préférée consiste à inclure le jeton unique dans un champ caché. Le jeton unique peut également être inclus dans l'URL ou un paramètre.
A9	Utilisation de composants avec des vulnérabilités connues	Les composants, tels que les bibliothèques, les Framework et les autres modules logiciels, fonctionnent avec les mêmes privilèges que l'application. Si un composant vulnérable est exploité, une telle attaque peut faciliter la perte sérieuse de données ou la prise de contrôle du serveur. Les applications et les API utilisant des composants présentant des vulnérabilités connues peuvent compromettre les défenses d'application et permettre diverses attaques et impacts.	Inventaire en continu des versions des composants du côté du client et du côté du serveur et de leurs dépendances. Utilisez des outils d'analyse de composition logicielle pour automatiser le processus. Déployer un correctif virtuel qui analyse le trafic HTTP, le flux de données ou l'exécution du code et empêche les vulnérabilités d'être exploitées.
A10	API sous-protégées	Les applications modernes impliquent souvent des applications et des API riches, telles que JavaScript dans le navigateur et les applications mobiles, qui se connectent à une API d'une certaine sorte .Ces API ne sont souvent pas protégées et contiennent de nombreuses vulnérabilités.	Assurez-vous que vous avez sécurisé les communications entre le client et vos API. Assurez-vous d'avoir un schéma d'authentification solide pour vos API et que toutes les informations d'identification. Implémentez un système de contrôle d'accès qui protège les API d'une mauvaise utilisation

Tableau 5 TOP 10 OWASP

- **La table suivante montre les différentes responsabilités du WAF :**

Type d'employée / Taches	IT Manager	Ingénieur de sécurité	Analyste des systèmes d'informations
Administration	R	R	C
Rapports de consultation	A	R	A
Déploiement	I	R	I
Tests	R	R	R

Tableau 6 Matrice RACI (WAF)

4. Wallix Admin Bastion (WAB) :

WALLIX propose des solutions logicielles de gestion des accès à privilèges pour les grandes et moyennes entreprises, organisations publiques et opérateurs de services cloud. Ces solutions aident leurs utilisateurs à protéger les actifs informatiques critiques y compris leurs données, serveurs, terminaux et objets connectés.

Wallix Admin Bastion Suite (ou WAB Suite) offre l'accès le plus direct vers la sécurité et la conformité en réduisant le risque le plus important – les accès à privilèges – dans le temps le plus court. [6]

- **Les fonctionnalités de WAB et leur bénéfice :**

Fonctionnalités	Descriptions	Bénéfices
Contrôle d'accès	WAB permet de définir une politique de contrôle d'accès très fine en fonction des critères suivants : applications et/ou serveurs cibles, comptes cibles, protocoles, plages horaires... WAB	Il est ainsi simple de savoir très précisément à quels comptes et quels équipements les utilisateurs peuvent accéder. Ainsi, il n'est plus nécessaire

	supporte les principaux protocoles utilisés pour l'administration des équipements et serveurs : HTTP/HTTPS, RDP/TSE, SSH, Telnet, VNC, SFTP…	d'ouvrir l'accès au système d'information plus que le strict nécessaire : les politiques de gestion des risques sont optimisées.
Authentification unique	Un seul identifiant et un seul mot de passe à retenir pour accéder à l'ensemble des comptes cibles autorisés - identifiant et mot de passe qui peuvent être les mêmes que ceux du compte annuaire de l'utilisateur.	Les administrateurs n'ont plus besoin de « cahier à mots de passe » et il n'est plus nécessaire de communiquer les mots de passe sensibles à l'extérieur de l'entreprise.
Accès aux applications métiers & clients/serveurs	WAB permet de tracer les accès, d'enregistrer les actions et d'effectuer une authentification unique (SSO) lors de l'accès à des applications métiers ou clients/serveurs telles que VMware ESX, Oracle, MySQL …	L'accès aux comptes à privilèges des applications métiers ou clients/serveurs est désormais aussi sécurisé et traçable que les accès aux comptes systèmes Windows ou Unix/Linux.
Traçabilité et enregistrement des sessions des utilisateurs à privilèges	Toutes les connexions effectuées sur les équipements cibles sont tracées et peuvent être enregistrées, qu'il s'agisse de sessions graphiques (RDP/TSE, VNC) ou de lignes de commande (SSH, Telnet).	Il est ainsi possible de savoir qui s'est connecté, quand, à quel compte cible, combien de temps puis de visionner l'enregistrement de la session pour analyser son contenu.
Coffre-fort à mot de passe	WAB peut modifier les mots de passe des équipements cibles, à la demande ou périodiquement.	Les exigences réglementaires en termes de changement et de durcissement des mots de passe des équipements critiques sont respectées sans avoir aucune conséquence sur le travail des équipes IT.
Fonctionnement sans agent	WAB fonctionne sans agent spécifique ni sur les équipements cibles, ni sur les postes de travail.	L'absence d'agent rend le déploiement, l'administration au quotidien et les mises à jour du WAB simples et rapides.
Statistiques et Rapports d'activité	Les statistiques et rapports sur l'activité du WAB sont disponibles dans l'interface d'administration	Les responsables de la sécurité des Systèmes d'Information ont une vision

	ainsi que via WAB Report Manager (WRM)*.	synthétique, qualitative et quantitative de l'activité des utilisateurs à privilèges.
Délégation d'administration	La gestion des profils permet de définir, pour chaque administrateur du WAB, les opérations d'administration autorisées (création d'utilisateurs, modification de droits ...).	Il est possible de définir des périmètres fonctionnels pour des administrateurs (ex. : Admin Unix, Admin Windows) et de créer des rôles spécifiques (ex. : profil « auditeur »).
Analyse du flux & OCR	Permet de détecter en temps réel des chaines de caractères dans les sessions SSH et d'analyser le contenu des sessions RDP/TSE.	Il est possible de connaître de façon très précise les actions réalisées dans une session SSH ou RDP/VNC.
Visualisation en temps réel	Permet à un administrateur du WAB de visualiser en temps réel le contenu des sessions RDP & SSH actives/ ouvertes sur le WAB et de les interrompre si nécessaire.	Il est ainsi possible de répondre aux problématiques réglementaires du type « 4 yeux ».
Support des services Web (SOAP) pour le provisionnement du WAB	Le provisionnement des utilisateurs, des comptes et équipements cibles, des droits d'accès peut être effectué dans le WAB via des services Web de type SOAP.	Cette synchronisation automatique entre une solution centrale de type IAM et un WAB permet de diminuer de façon drastique le TCO du WAB

Tableau 7 Les fonctionnalités de WAB et leur bénéfice

- **La table suivante montre les différentes responsabilités du WAB :**

Type d'employée / Taches	IT Manager	Ingénieur de sécurité	Analyste des systèmes d'informations
Administration	R	R	C
Rapports de consultation	A	R	A
Déploiement	I	R	I
Tests	R	R	R

Tableau 8 Matrice RACI (WAB)

Conclusion :

Nous avons introduit dans ce chapitre la notion de la sécurité informatique. Puis nous avons présenté l'organisme d'accueil et décrit son architecture, d'où, le chapitre suivant est consacré à l'étude de la série ISO/IEC 2700x et la notion du SMSI.

Chapitre 2

La série des normes ISO/ IEC 27000

L'objectif de ce chapitre est de faire une étude sur les normes et référentiel de sécurité des systèmes d'information et ensuite présenter la famille des normes ISO/IEC 27000.

I. Vue globale sur les normes et les référentiels de sécurité de l'information :

L'objectif de ce chapitre est de présenter les normes et les référentiels, les concepts, les processus et les acteurs qui ont permis aux organismes d'aboutir à la continuité de la sécurité de l'information.

1. Les normes :

1. Définition :

L' Organisation International de Standardisation (ISO) donne la définition suivante d'une norme : « document, établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné». Une norme est donc un document de référence, obtenu par consensus et approuvé par un organisme de normalisation.

Les organismes de normalisation sont présents au plan national ainsi que AFNOR en France (norme NF), au niveau européen avec le Comité Européen de Normalisation (norme CEN) et au niveau international avec l'Organisation International de Standardisation (norme ISO).

La normalisation internationale est désormais un fait acquis pour de nombreuses technologies et pour des secteurs très variés. Fin 2006, près de 16 000 normes actives étaient recensées par l'ISO. Beaucoup sont intégrées à la vie courante comme la sensibilité ISO des pellicules ou la norme relative aux formats de papier (ISO 216).

En informatique, citons l'ISO 9660 pour le système de fichiers sur CD-ROM, l'ISO 9899 pour le langage C ou encore le modèle OSI en 7 couches (ISO 7498).

Parmi les normes les plus connus en matière de sécurité de l'information PCI DSS et La série de norme ISO/IEC 27000. [7]

2. PCI DSS :

Le Conseil des normes de sécurité PCI est un forum international ouvert pour le développement, l'amélioration, le stockage, la diffusion et la mise en œuvre en continu de normes de sécurité pour la protection des données de comptes.

La mission du Conseil des normes de sécurité PCI est d'améliorer la sécurité des données des comptes de paiement en favorisant l'éducation et la sensibilité aux normes de sécurité PCI. L'organisation a été fondée par American Express, Discover Financial Services, JCB International, MasterCard et Visa, Inc. [7]

NB : Le PCI-DSS est destiné au secteur des banques et la sécurité des cartes magnétiques.

3. ISO/IEC 27001

ISO / IEC 27001 définit formellement un système de gestion de la sécurité de l'information (SMSI), une suite d'activités concernant la gestion des risques d'information (appelés «risques de sécurité de l'information» dans la norme). Le SMSI est un cadre de gestion global par lequel l'organisation identifie, analyse et résout ses risques d'information. Le SMSI garantit que les arrangements de sécurité sont adaptés pour suivre les changements apportés aux menaces, aux vulnérabilités et aux impacts sur les risques liés à la sécurité.

NB : ISO / IEC 27001 est destinée à n'importe quelle type et n'importe quelle taille d'entreprise et donne la possibilité d'avoir un certificat.

2. Les référentiels :

Un référentiel c'est tout simplement un ensemble d'éléments auxquels on se compare ; il répond à un besoin de standardisation autour d'un vocabulaire commun. Il peut s'agir de standards ou de normes encore appelées standard de jure.

1. Cobit :

La nécessité d'avoir un cadre de référence en matière de sécurité et de contrôle des technologies de l'information a poussé l'ISACA (Information Systems Audit and Control Association) à créer la méthode COBIT en 1996. Cette méthode est diffusée en France par sa branche française l'AFAI (Association Française de l'Audit et du Conseil Informatique).

L'objectif était de faire le lien entre les risques métiers, les besoins de contrôle et les questions techniques en se basant sur les meilleures pratiques en audit informatique et SI.

Le COBIT se destine aussi bien au management (qui doit décider des investissements à effectuer pour assurer la sécurité et la maîtrise des TI, et les ajuster suivant les risques de l'environnement) qu'aux utilisateurs (sécurité, mise sous contrôle des services informatiques

fournis). La méthode COBIT se veut le modèle de référence de la gouvernance des TI.

La version 5 de COBIT est disponible depuis avril 2012 COBIT 5 est, à ce jour, le seul référentiel qui est orienté business pour la Gouvernance et la Gestion des Systèmes d'Information de l'entreprise. Il représente une évolution majeure du référentiel. COBIT 5 peut être adapté pour tous les types de modèles business, d'environnements technologiques, toutes les industries, les lieux géographiques et les cultures d'entreprise. Il peut s'appliquer à :

- La sécurité de l'information
- La gestion des risques
- La gouvernance et la gestion du Système d'Information de l'entreprise
- Les activités d'audit
- La conformité avec la législation et la réglementation
- Les opérations financières ou les rapports sur la responsabilité sociale de l'entreprise [8]

NB : Le référentiel COBIT 5 simplifie les défis de la gouvernance et il permet l'intégration avec d'autres approches et normes, incluant ISO 27001, ITIL, PCI DSS mais ce n'est pas gratuit et non disponible au sein d'UNIDEES.

2. ITIL :

C'est un référentiel de bonnes pratiques en matière de gestion du système d'information. ITIL est devenu le standard en matière de gestion des services.

Origines : ITIL a été initialement développé dans les années 80 sous la pression du gouvernement de Margaret Thatcher pour optimiser les prestations informatiques internes. Composé à l'origine de plusieurs dizaines d'ouvrages, ce référentiel a évolué pour s'adapter à l'évolution des technologies de l'information.

La bibliothèque : Dans sa version actuelle, ITIL est composé de huit ouvrages :

- The business perspective (point de vue de l'entreprise).
- Application management (gestion des applications).
- ICT infrastructure management (gestion des infrastructures informatiques).

- Planning to implement service management (planification et mise en œuvre de la gestion des services).
- Service delivery (fourniture des services).
- Service support (soutien en matière de services).
- Security management (gestion de la sécurité).
- Software asset management (gestion des assets logiciels)

Les avantages d'ITIL : Au moment où chacun tente de progresser sur l'optimisation des processus dont il a la responsabilité, ITIL apporte les bases d'une production informatique structurée pour répondre à des exigences de qualité et de productivité de plus en plus fortes. En outre, à travers le processus de gestion des niveaux de services, ITIL accompagne le projet de contractualisation des services entre la DSI et les directions utilisatrices. [7]

NB : Le référentiel ITIL est destiné beaucoup plus aux entreprises de production.

3. Choix important :

Selon les informations prédicants et notre recherche sur les normes et les référentiels les plus utilisé aux monde d'IT on a vu qu'ils sont inspirée depuis la famille des normes ISO/IEC 27000, la meilleure façon pour garantir l'amélioration continue de la sécurité de l'information chez UNIDEES est d'implémenter le SMSI de la série des normes ISO/CEI 27000 et d'avoir en plus un certificat de conformité à la norme ISO/CEI 27001.

II. La famille des normes ISO/IEC 27000 :

1. ISO & IEC :

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent à l'élaboration de Normes internationales par l'intermédiaire de comités techniques créés par l'organisme concerné pour traiter du domaine particulier à une activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organismes internationaux, gouvernementaux et non gouvernementaux, en liaison avec l'ISO et l'IEC participent également aux travaux. Dans le domaine des technologies de l'information,

En 1987, l'ISO et le IEC créent le Joint Technical Committee (JTC1) pour la normalisation des Technologies de l'Information (TI). Le JTC1 allie les compétences de l'ISO en matière de langage de programmation et codage de l'information avec celles du CEI qui traitent du matériel tel que les microprocesseurs. Le JTC1 est composé de plusieurs comités techniques (SC) qui traitent des sujets tels que la biométrie, la téléinformatique, les interfaces utilisateurs ou encore les techniques de sécurité de l'information relatives aux normes de la série ISO/CEI 2700x. [9]

2. Historique des normes en matière de sécurité de l'information

Au cours des vingt dernières années les normes liées à la sécurité de l'information ont évolué ou ont été remplacées. Ces changements rendent difficile une bonne compréhension du sujet. Un rappel historique de l'évolution de ces normes permet de clarifier la situation normative en matière de sécurité de l'information.

Au début des années 90, de grandes entreprises britanniques se concertent pour établir des mesures visant à sécuriser leurs échanges commerciaux en ligne. Le résultat de cette collaboration servit de référence en la matière pour d'autres entreprises qui souhaitaient mettre en œuvre ces mesures. Cette initiative privée fut appuyée par le Département des Transports et de l'Industrie britannique qui supervisa la rédaction au format du BSI, d'une première version de projet de norme de gestion de la sécurité de l'information.

En 1991, un projet de «best practices» code de bonnes pratiques, préconise la formalisation d'une politique de sécurité de l'information. Cette politique de sécurité doit intégrer au minimum huit points «stratégique et opérationnel» ainsi qu'une mise à jour régulière de la politique.

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

En 1998, la norme BS7799 change de numérotation et devient la norme BS7799-1. Elle est complétée par la norme BS7799-2 qui précise les exigences auxquelles doit répondre un organisme pour mettre en place une politique de sécurité de l'information. Cette nouvelle norme est fondée sur une approche de la maîtrise des risques et sur le principe du management de la sécurité de l'information.

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

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

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

En 2007, dans un souci de clarification, l'ISO renomme la norme ISO/IEC 17799 :2005 en changeant sa numérotation pour ISO/IEC 27002. La norme se greffe à la famille des normes ISO/IEC 2700x toujours en développement.

En 2013, une révision de la norme ISO/IEC 27001 et ISO/ IEC 27002.

En 2016, une révision de la norme ISO/IEC 27000 et ISO/ IEC 27004.

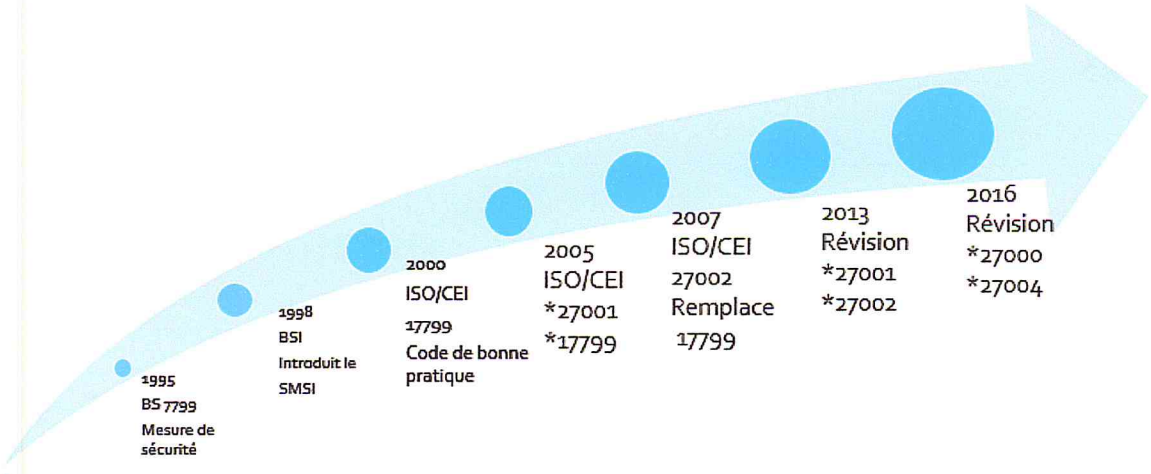


Figure 4 Résumé de l'historique des normes de sécurité

Aujourd'hui les organismes disposent de deux normes qui se sont imposées comme référence des SMSI, l'ISO/CEI 27001 :2005 qui décrit les exigences pour la mise en place d'un SMSI et

l'ISO/CEI 27002 qui regroupe un ensemble de bonnes pratiques «best practices» pour la gestion de la sécurité de l'information.

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

Dans la partie qui suit nous présentons les principales propriétés d'un SMSI avant d'aborder les normes de la série ISO/CEI 2700x qui se sont imposées comme références des SMSI.

3. Les SMSI (Systèmes de Management de la Sécurité de l'Information)

La norme ISO 9000 définit le système de management comme : « un système permettant d'établir une politique, des objectifs et éventuellement la possibilité d'atteindre ces objectifs ».

Un système de management peut être interprété comme un ensemble de mesures organisationnelles et techniques ciblant un objectif comme le montre la figure 5 ci-dessous [9]

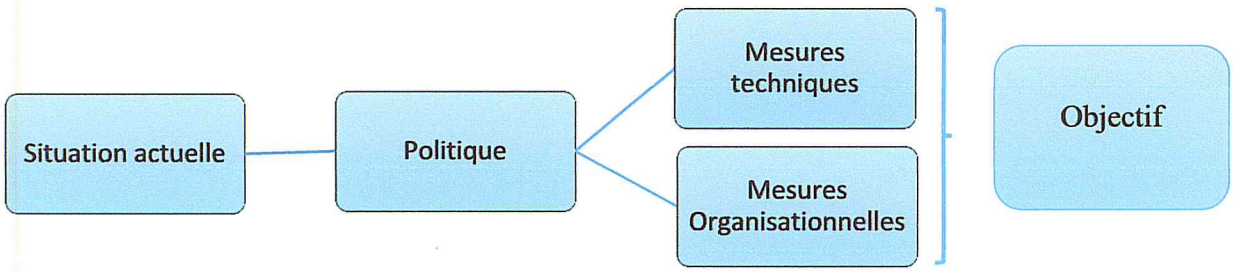


Figure 5 Vue d'un système de management

4. La famille des normes ISO/IEC 2700x :

Dans la famille ISO/CEI on trouve deux catégories de normes. Celles qui émettent des exigences : ISO/CEI 27001 et celles qui formulent des recommandations : ISO/CEI 27002. Notons que certaines normes sont encore en cours de rédaction.

Comme représenté sur la figure 6 ci-dessous, la norme ISO/CEI 27001 est le centre de gravité des référentiels du SMSI. La norme ISO/CEI 27001 formule les exigences relatives aux SMSI et fournit une liste de mesures de sécurité pouvant être intégrées au système.

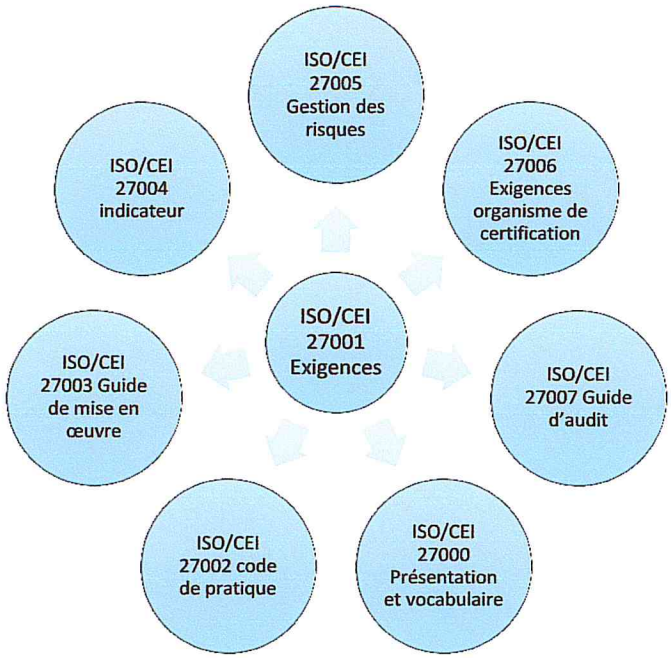


Figure 6 Le centre de gravité de série des normes 27000

1) L'ISO/CEI 27000

Cette norme a été publiée pour répondre au besoin de définir une terminologie pour les SMSI. Comme nous l'avons vu précédemment, beaucoup de référentiels antérieurs à ISO/CEI 27001 ont été publiés ces dernières années. Ces normes ne fournissent pas de notions, ni de vocabulaire commun, permettant une bonne compréhension des SMSI, c'est ce que propose l'ISO/CEI 27000.

L'ISO/CEI 27000 est structurée en trois parties. La première, définit 46 termes tels que, la confidentialité, l'intégrité, la disponibilité, l'authenticité, tous principalement axés sur l'appréciation et l'analyse des risques, des menaces, de la vulnérabilité, etc. Par exemple, le mot risque est « la combinaison de la probabilité d'un événement et de ses conséquences ».

La deuxième partie développe la notion de processus avec le modèle PDCA et présente les concepts propres aux SMSI comme par exemple, l'importance de l'engagement de la direction.

La troisième partie, est une présentation de l'ensemble des normes de la famille ISO/CEI 2700x. [9]

2) L'ISO/CEI 27001

ISO / IEC 27001 définit formellement un système de gestion de la sécurité de l'information (SMSI), une suite d'activités concernant la gestion des risques d'information (appelés «risques de sécurité de l'information» dans la norme). Le SMSI est un cadre de gestion global par lequel l'organisation identifie, analyse et résout ses risques d'information. Le SMSI garantit que les arrangements de sécurité sont adaptés pour suivre les changements apportés aux menaces, aux vulnérabilités et aux impacts sur les risques liés à la sécurité.

La norme couvre tous les types d'organisations (par Exemple : Entreprises commerciales, agences gouvernementales, sans but lucratif), toutes les tailles (des microentreprises aux multinationales énormes) et toutes les industries ou marchés (par exemple : commerce de détail, banque, défense, santé, éducation Et le gouvernement).

L'ISO / CEI 27001 ne prescrit pas officiellement des contrôles spécifiques de la sécurité de l'information, car les contrôles requis varient considérablement selon le large éventail d'organisations adoptant la norme. Les contrôles de sécurité de l'information de l' ISO / CEI 27002 sont indiqués dans l'annexe A de l'ISO / CEI 27001, plutôt qu'un menu. Les organisations adoptant ISO / IEC 27001 sont libres de choisir les contrôles spécifiques de sécurité de l'information applicables à leurs risques particuliers en matière d'information, en s'appuyant sur ceux énumérés dans le menu et en les complétant potentiellement par d'autres options à la carte (parfois appelées jeux de contrôle étendus).

Statut de la norme

L'ISO / CEI 27001 a été entièrement réécrit et réémis en septembre 2013. C'était bien plus que simplement peaufiner le contenu de l'édition 2005 puisque l'ISO / CEI JTC1 a insisté sur des changements substantiels pour aligner cette norme avec d'autres normes de systèmes de gestion couvrant l'assurance de la qualité, la protection de l'environnement, etc.

Remarque :

ISO/IEC 27001 Est une spécification pour la création d'un SMSI. Il ne prescrit pas de mesures précises, mais comprend des suggestions de documentation, des audits internes, une amélioration continue et des mesures correctives et préventives.

Comme avec tous les processus de gestion, un SMSI doit rester efficace et efficace à long terme, en s'adaptant aux changements dans l'organisation interne et l'environnement externe. L'ISO / CEI 27001 : 2005 a donc incorporé l'approche «Plan-Do-Check-Act» (PDCA) ou «Deming cycle».

Après la révision de la norme en 2013, la norme 27001 ne met plus l'accent sur le cycle Deming. L'utilisateur SMSI est libre d'utiliser toute approche de processus de gestion (amélioration) comme PDCA, Six Sigmas, Les cercles de la qualité….etc.

Les méthodes qui assurent la continuité de sécurité des SI :

PDCA :

La roue de Deming (de l'anglais Deming wheel) est une illustration de la méthode de gestion de la qualité dite PDCA (plan-do-check-act).

Plan (établissement du SMSI) : Établir la politique, les objectifs du SMSI, les processus et procédures liés à la gestion des risques et l'amélioration de la sécurité de l'information afin de fournir des résultats conformes aux politiques et aux objectifs globaux de l'organisation.

Do (mise en œuvre et fonctionnement du SMSI) : Mettre en œuvre et exploiter la politique, les contrôles, les processus et les procédures du SMSI.
Check (suivi et examen du SMSI : Évaluer et, le cas échéant, mesurer les performances des processus par rapport à la politique, les objectifs et l'expérience pratique et rendre compte à la direction pour examen.

Act (mise à jour et amélioration du SMSI) : Prendre des mesures correctives et préventives, sur la base des résultats de la vérification interne du SMSI et de l'examen de la direction, ou d'autres informations pertinentes pour améliorer continuellement ledit système.

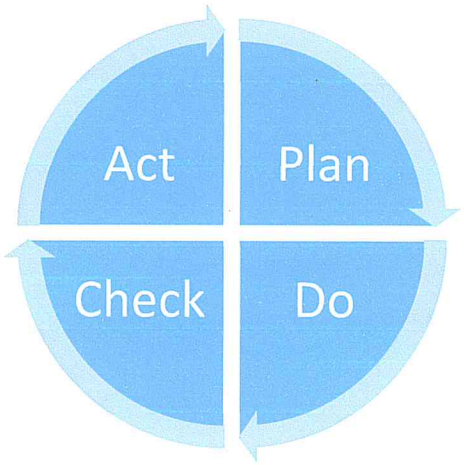


Figure 7 Présentation de la procédure PDCA

La Méthode Six Sigma :

(États-Unis) Six Sigma méthode de management visant à l'amélioration permanente de la qualité. Equivalent : PDCA, dont elle est une version améliorée.

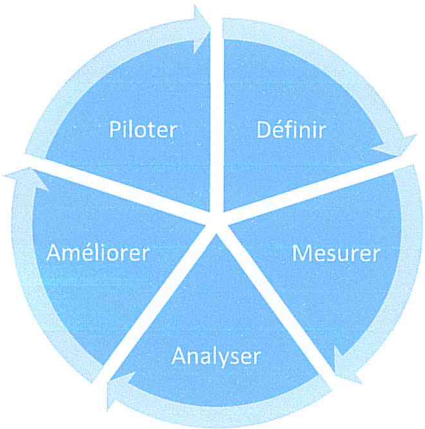


Figure 8 Présentation de la procédure Six Sigma

Les cercles de la qualité :

Les cercles de la qualité sont principalement des outils de communication. Ils ont pour but de partager l'information, d'améliorer la qualité du travail, de favoriser la compréhension des objectifs et la reconnaissance mutuelle. Pour qu'ils fonctionnent, il faut 3 conditions :

- Qu'il existe une vraie envie d'amélioration et donc un sens des responsabilités
- Qu'il y ait un climat de confiance et donc une transparence dans la conduite des actions, bref une lisibilité du management

- Que puisse se manifester l'esprit critique, c'est à dire qu'il n'y ait pas d+e sentiment de culpabilité. Ils peuvent voir le jour sous plusieurs formes :
    - Propre à l'unité de travail ou transversal
    - Permanent ou temporel
    - Etre à l'initiative de la hiérarchie

Choix important :

Selon les informations prédicants, la meilleure méthode pour garantir l'amélioration de la sécurité de l'information chez UNIDEES, et la richesse de documentation sur la méthode PDCA on a choisi de travailler avec cette dernière.

La structure de la norme (Version 2013) :

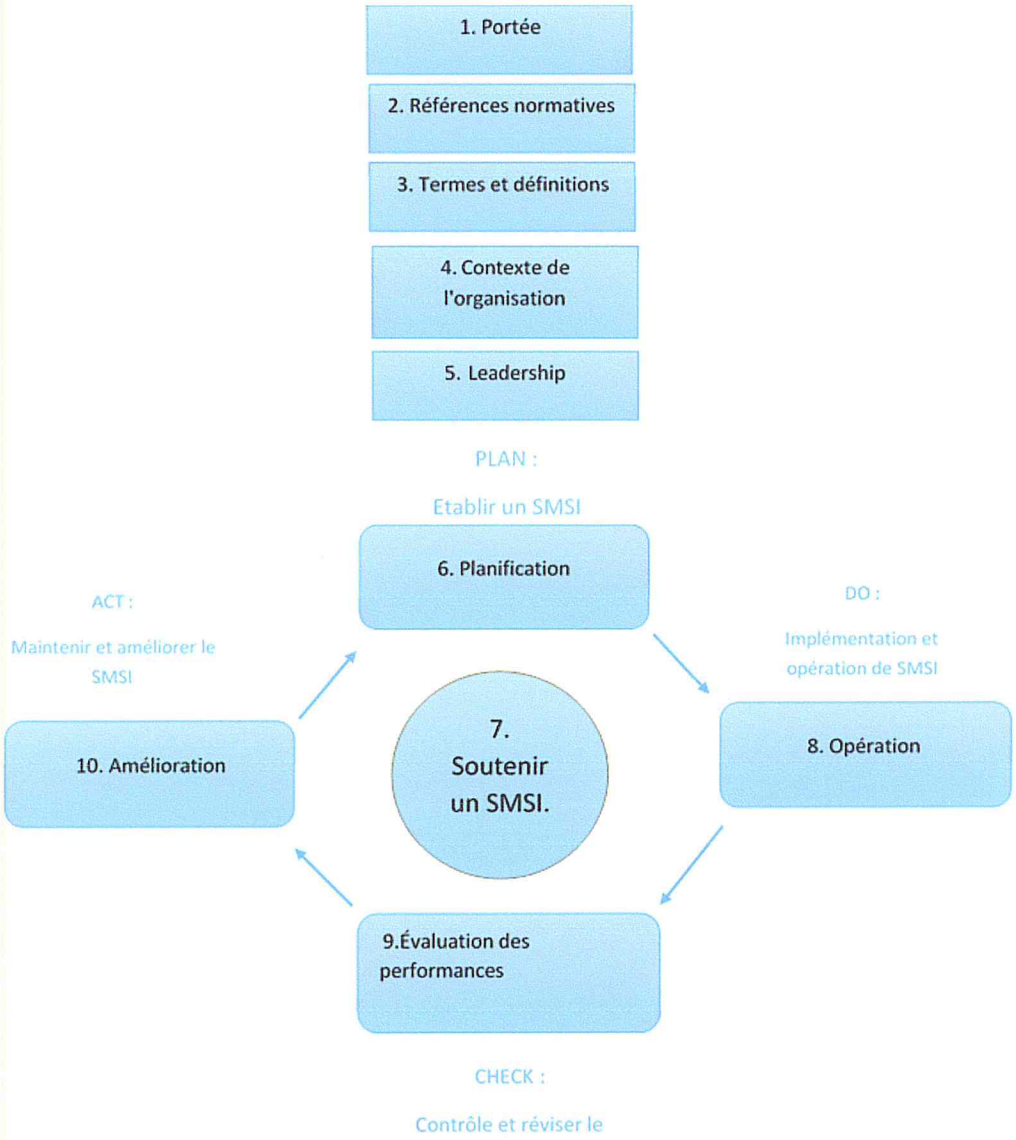


Figure 9 Structure de la norme ISO/IEC 27001 avec la méthode PDCA

1. Portée :

La première clause détaille la portée de la norme.

2. Références normatives :

Toutes les références normatives sont contenues dans la norme ISO / CEI 27000, Technologies de l'information - Techniques de sécurité - Systèmes de gestion de la sécurité de l'information - Vue d'ensemble et vocabulaire, référencées et précieuses.

3. Termes et définitions :

Veuillez-vous référer aux termes et définitions contenus dans la norme ISO / CEI 27000. Il s'agit d'un document important à lire.

4. Contexte de l'organisation :

Ceci est la clause qui établit le cadre de l'organisation et les effets sur le SMSI. Une grande partie du le reste de la norme a trait à cette clause.

Le point de départ est d'identifier toutes les questions internes et externes pertinentes à votre organisation et vos informations ou des informations est confiée à vous par les parties tierces.

Ensuite, vous devez établir toutes « Les parties intéressées » et les parties prenantes, ainsi que la façon dont elles sont pertinentes pour l'information. Vous aurez besoin d'identifier les besoins des parties intéressées qui pourrait inclure des obligations juridique, réglementaire et / ou contractuelle. Vous aurez également besoin de considérer des sujets tels que l'assurance de tout le marché et les objectifs de gouvernance comme importants.

Vous devrez décider de la portée de votre SMSI, qui doit faire le lien avec l'orientation stratégique de votre organisation, les objectifs fondamentaux et les exigences des parties intéressées.

Enfin, vous devez montrer comment vous allez établir, mettre en œuvre, maintenir et améliorer sans cesse le SMSI par rapport à la norme.

5. Leadership :

L'article 5 énumère un certain nombre d'exigences pour les cadres supérieurs pour assurer le leadership et l'engagement à la mise en œuvre des SMSI. Il définit également le terrain pour la documentation d'une politique de sécurité de l'information et l'identification des responsabilités et des pouvoirs des rôles pertinents à la sécurité de l'information.

6. Soutenir un SMSI :

Cette section de l'ISO / CEI 27001 vise à obtenir les bonnes ressources, les bonnes personnes et la bonne infrastructure en place pour établir, mettre en œuvre, maintenir et améliorer continuellement le SMSI. Il traite des exigences en matière de compétence, de sensibilisation et de communication à l'appui du SMSI et pourrait, par exemple, faire en sorte que la formation et le personnel soient disponibles.

Cette clause exige également que tout le personnel travaillant sous le contrôle d'une organisation soit au courant de la politique de sécurité de l'information, de façon à contribuer à son efficacité et de gérer les conséquences de non-conformité.

L'organisation doit également veiller à ce que les communications internes et externes pertinentes à la sécurité de l'information et au SMSI soient correctement communiquées. Cela comprend l'identification de ce qui doit être communiqué à qui, quand et comment cela est livré.

C'est dans cet article que le terme «information documentée» est référencé. Les organisations doivent déterminer le niveau des informations documentées qui sont nécessaires pour contrôler le SMSI.

On met également l'accent sur le contrôle de l'accès à l'information documentée, ce qui reflète l'importance de la sécurité de l'information.

7. Planification (PLAN) :

Cet article décrit les plans d'organisation des mesures visant à faire face aux risques et information.

Il se concentre sur la façon dont une organisation traite Sécurité de l'information et doit être Proportionnel à l'impact potentiel qu'elles ont.

ISO 27005, la norme internationale pour la Gestion des risques, contient des orientations précieuses.

Les organisations sont également tenues de «Déclaration d'applicabilité» (SoA). Le SoA fournit un résumé des décisions prises par une organisation en matière de traitement des risques, des objectifs et des contrôles que vous avez inclus, ceux que vous avez et pourquoi vous avez décidé d'inclure et d'exclure les contrôles dans la SoA.

Un autre domaine clé de cet article est la nécessité de déterminer les objectifs de sécurité de l'information et de définir les propriétés que la sécurité de l'information doit avoir.

8. Opération « DO » :

Cet article porte sur l'exécution des plans et des processus qui font l'objet des clauses précédentes. Il traite de l'exécution des actions déterminées et de la réalisation des objectifs de sécurité de l'information. En reconnaissance de l'utilisation accrue des fonctions externalisées dans le monde des affaires d'aujourd'hui, ces processus doivent également être identifiés et

contrôlés. Tout changement, qu'il soit planifié ou non, doit être pris en considération ici et les conséquences de celles-ci sur le SMSI. Il traite également de l'exécution des évaluations des risques liés à la sécurité de l'information à intervalles prévus et de la nécessité de conserver des informations documentées pour en consigner les résultats. Enfin, il y a une section qui traite de la mise en œuvre du plan de traitement des risques et, encore une fois, la nécessité que les résultats de ces derniers soient conservés dans des informations documentées.

9. Évaluation des performances « CHECK » :

Cet article traite de la surveillance, de la mesure, de l'analyse et de l'évaluation de votre SMSI afin de s'assurer qu'il est efficace et qu'il l'est toujours. Cette clause aide les organisations à évaluer continuellement leur performance par rapport aux objectifs de la norme afin de s'améliorer continuellement.

Vous devrez considérer les informations dont vous avez besoin pour évaluer l'efficacité de la sécurité de l'information, Les méthodes employées et le moment adéquat pour l'analyse et le signalement.

Des audits internes devront être effectués ainsi que des examens de la direction. Les deux doivent être effectués à des intervalles prévus et les résultats devront être conservés en tant qu'informations documentées.

Il convient de noter que les examens de la gestion sont également l'occasion d'identifier les domaines à améliorer.

10. Amélioration « ACT » :

Cette partie de la norme concerne les mesures correctives requises. Vous aurez besoin de montrer comment vous réagissez aux non-conformités, de prendre des mesures, de les corriger et de traiter les conséquences. Vous devrez également montrer si des non-conformités semblables existent ou pourraient potentiellement se produire et montrer comment vous allez éliminer les causes de ces non-conformités afin qu'elles ne se reproduisent pas ailleurs.

Il est également nécessaire de faire preuve d'une amélioration continue du SMSI, notamment en démontrant l'adéquation de celui-ci et son efficacité. Cependant l'accomplissement de cette tâche revient à l'utilisateur.

L'ISO / CEI 27001 comprend également l'annexe A qui décrit 114 contrôles pour aider à protéger l'information dans une variété de domaines à travers l'organisation. L'ISO / CEI 27002 fournit également des conseils sur les meilleures pratiques et constitue une référence

précieuse pour le choix et l'exclusion des contrôles les mieux adaptés à votre organisation. [10]

Statistique d'utilisation de la norme ISO/IEC 27001 dans le monde :

Les trois pays en tête de classement pour le nombre total des certifications ISO/CEI 27001 sont le Japon, l'Inde et le Royaume-Uni, la progression la plus forte de la certification dans ce domaine étant enregistrée au Japon, en Roumanie et en Chine.

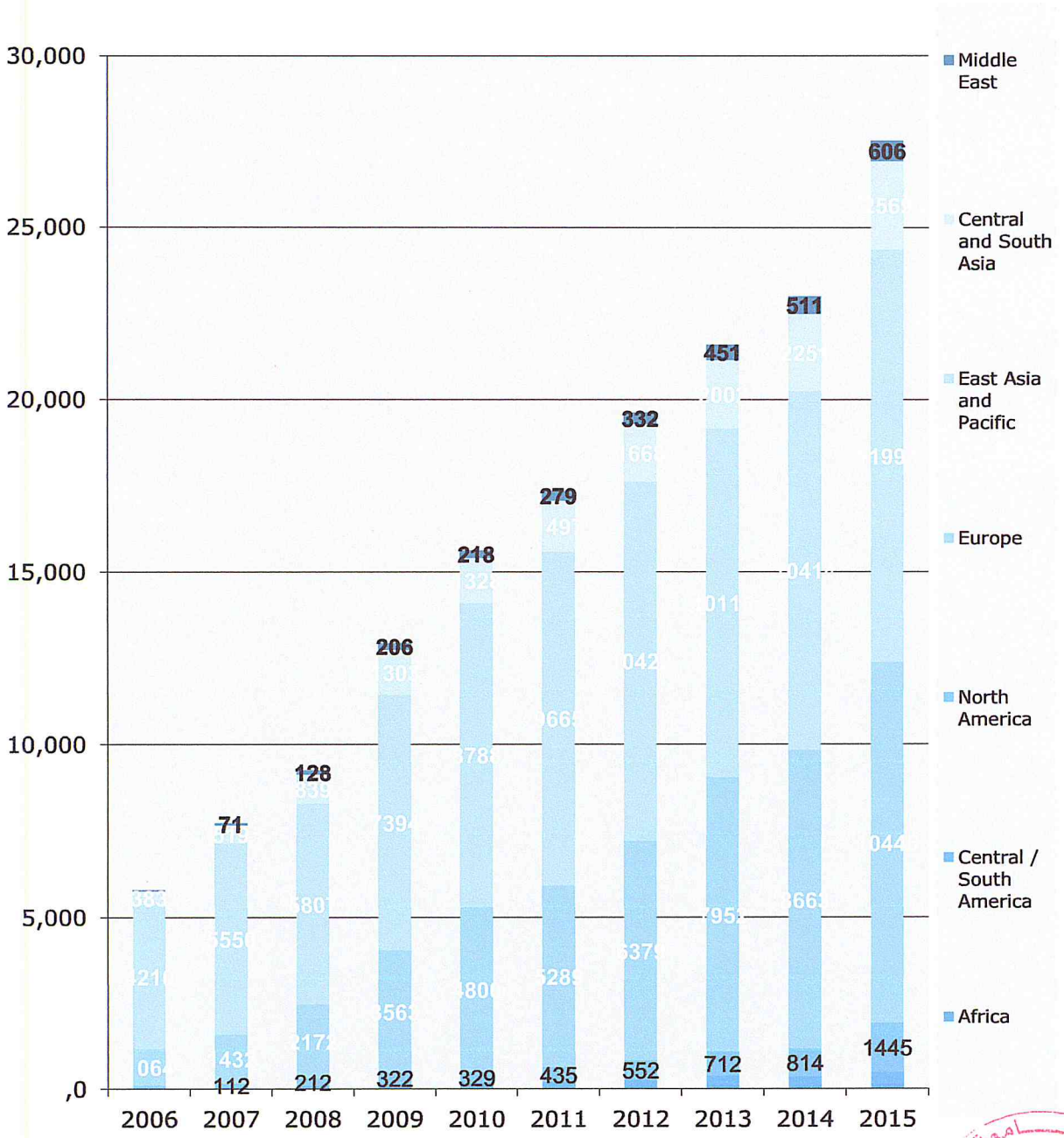


Figure 10 Statistique sur l'utilisation de l'ISO/IEC 27001 [17]

3) L'ISO/CEI 27002

ISO / IEC 27002 est un standard de bonnes pratiques reconnu internationalement pour la sécurité de l'information. ISO / IEC 27002 retrace son histoire plus de 30 ans aux précurseurs de BS 7799.

La norme propose sur onze chapitres, une liste de 133 mesures de sécurité accompagnées chacune de points à aborder pour la mise en place d'un SMSI. L'ISO/CEI 27002 est un guide de bonnes pratiques, une série de préconisations concrètes, abordant les aspects tant organisationnels que techniques, qui permettent de mener à bien les différentes actions dans la mise en place d'un SMSI.

La norme est actuellement en cours de révision pour refléter les changements dans la sécurité de l'information. Deux approches sont actuellement envisagées en parallèle :

1. Les contrôles seront regroupés en «thèmes» formant des clauses dans le corps principal de la norme
2. Le corps principal de la norme offrira plusieurs «vues» signifiant diverses classifications ou regroupements de contrôles de sécurité de l'information selon leurs balises, les contrôles. [11]

Statut de la norme :

La version révisée de l'ISO / CEI 27002 a été publiée en septembre 2013 en même temps que la version mise à jour de l'ISO / CEI 27001. La décision de laisser tomber la définition de «l'actif de l'information» à partir de la version actuelle de l'ISO / CEI 27000 plutôt que d'aboutir vraiment sur ce problème peut s'avérer être une erreur tactique. Un rectificatif technique publié en octobre 2014 a apporté des modifications mineures au libellé de l'ISO / CEI 27002 : 2013 pour clarifier que «l'information» est en effet un «actif».

4) L'ISO/CEI 27003

ISO / IEC 27003: 2010 se concentre sur les aspects critiques nécessaires pour la conception réussie et la mise en œuvre d'un système de gestion de sécurité de l'information (SMSI) conformément à la norme ISO / IEC 27001: 2013.

Il décrit le processus de spécification SMSI et la conception de la création à la production de plans de mise en œuvre, et le processus d'obtention de l'approbation de la direction pour mettre en œuvre un SMSI, définit un projet visant à mettre en œuvre un SMSI(visées à l'ISO /

IEC 27003: 2010 en tant que projet SMSI), et fournit des indications sur la façon de planifier le projet SMSI, résultant en un plan final de mise en œuvre du projet SMSI.

La norme ISO / CEI 27003 est un document de 78 pages comprenant 9 chapitres :

- Introduction (Chapitres 1 à 3)
- Le synoptique d'un SMSI (chapitre 4)
- L'approbation du projet SMSI (chapitre 5)
- Le Séquencement de la phase PLAN (Chapitres 6, 7, 8)
    - Posture de contribution au business et Périmètre : «SMSI scope»
    - Objectifs, Critères d'appréciation du risque : «SMSI Policy»
    - L'analyse de risque brut et net (couverture existante des Vulnérabilités.)
    - Instruire les mesures de sécurité (réduction du risque) applicables
    - Décision de traitement du risque et cible de risque résiduel, et la déclaration d'applicabilité
- La préparation de l'Implémentation de la phase DO (chapitre 9). [12]

Statut de la norme

La norme a été initialement publiée en 2010, en conseillant sur la façon de planifier un projet de mise en œuvre du SMSI. Elle a été considérablement révisée et rééditée en avril 2017 et reflète maintenant et explique la structure et la séquence de l'ISO / CEI 27001 : 2013 . Il ne prévoit plus une structure ou une approche de projet particulière.

5) L'ISO/CEI 27004

ISO / CEI 27004 concerne les mesures nécessaires pour la gestion de la sécurité de l'information ces informations sont communément appelées «mesures de sécurité» dans la profession. La norme est destinée à aider les entreprises à évaluer l'efficacité de leurs systèmes de gestion de la sécurité de l'information ISO27k, en fournissant les informations nécessaires pour gérer et améliorer systématiquement le SMSI. Il se développe de manière substantielle sur la clause 9.1 de l'ISO / CEI 27001 concernant le «suivi, la mesure, l'analyse et l'évaluation». [13]

Contenue de la norme :

Ce sont les principales sections :

5. Raison d'être - explique la valeur de la mesure, par exemple pour accroître la responsabilisation et la performance ;
6. Caractéristiques - Ce qu'il faut mesurer, surveiller, analyser et évaluer, quand le faire, et à qui le faire ;
7. Types de mesures - mesures de performance et efficacité ;
8. Processus - comment développer, mettre en œuvre et utiliser des mesures.

L'Annexe A est l'endroit où la plupart du modèle de mesure théorique de la version 2009 de la norme maintenant languit.

Catalogues de l'Annexe B 35 mesures d'exemples d'utilité et de qualité variables, en utilisant un formulaire de définition de métrique typique.

L'annexe C démontre une manière pseudo-mathématique de décrire une métrique, ou plutôt une «construction de mesure de l'efficacité».

Statut de la norme

La norme a été publiée pour la première fois en 2009. Une deuxième édition substantiellement révisée a été publiée en décembre 2016.

6) L'ISO/CEI 27005

La norme «fournit des lignes directrices pour la gestion du risque de sécurité de l'information» et elle «prend en charge les concepts généraux spécifiés dans ISO / IEC 27001 et est conçue pour aider à la mise en œuvre satisfaisante de la sécurité de l'information basée sur une approche de gestion des risques».

La norme ne spécifie et ne recommande aucune méthode de gestion des risques spécifique. Cela implique néanmoins un processus continu consistant en une séquence structurée d'activités, dont certaines sont itératives :

- Établir le contexte de la gestion des risques (par exemple, la portée, les obligations de conformité, les approches / méthodes à utiliser et les politiques et critères pertinents tels que la tolérance au risque ou l'appétit de l'organisation) ;
- Évaluer quantitativement ou qualitativement (c.-à-d. Identifier , analyser et évaluer) les risques d'information pertinents, en tenant compte des actifs d'information, des menaces, des contrôles existants et des vulnérabilités afin de déterminer la probabilité d'incidents

ou de scénarios incidents et les conséquences commerciales prévues s'ils se produiraient, Pour déterminer un «niveau de risque»;

- Traiter (c'est-à-dire modifier [utiliser les contrôles de sécurité de l'information], conserver [accepter], éviter et / ou partager [avec des tiers]) les risques de manière appropriée, en utilisant ces «niveaux de risque» pour les hiérarchiser ;
- Tenir les parties prenantes informées tout au long du processus ; et
- Surveillez et révisez les risques, les traitements de risque, les obligations et les critères de manière continue, en identifiant et en répondant de manière appropriée à des changements importants. [14]

Statut de la norme

La deuxième édition de l'ISO / CEI 27005 a été publiée en 2011. Il reflète la norme générale de gestion des risques de l'entreprise ou de l'entreprise ISO 31000 : 2009 « Gestion des risques - Principes et directives» dans le contexte spécifique des risques ou de l'information.

Un projet de révision de la norme conforme aux versions 2013 des ISO / CEI 27001 et 27002 a fait des progrès insuffisants et a été annulé et redémarré.

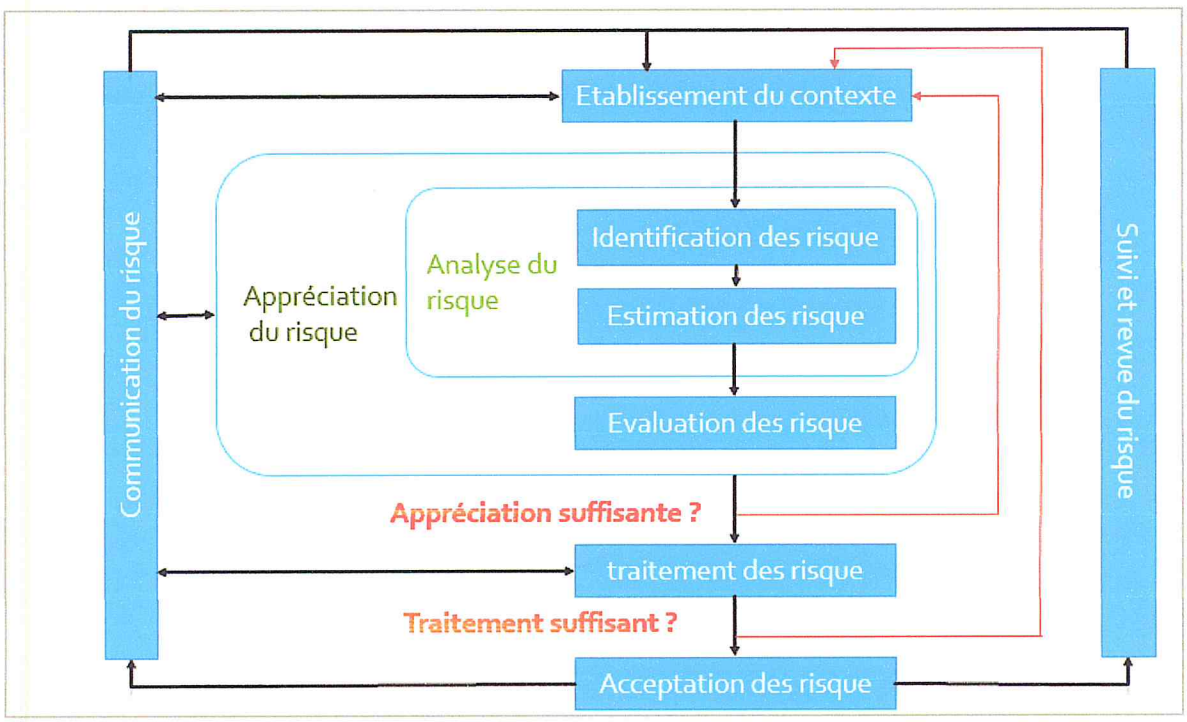


Figure 11 Procédure de gestion des risques [14]

7) L'ISO/CEI 27006

La portée de la norme ISO / CEI 27006 est de "spécifier les exigences et fournir des conseils pour les organismes fournissant l'audit et la certification d'un système de gestion de la sécurité de l'information (SMSI), en plus des exigences contenues dans ISO / CEI 17021 et ISO / CEI 27001. C'est Principalement destiné à soutenir l'accréditation des organismes de certification fournissant la certification SMSI ".

L'ISO / CEI 27006 spécifie les exigences et fournit des conseils pour l'audit de conformité spécifiquement dans le contexte des SMSI, en plus des exigences générales d'accréditation établies par ISO / CEI 17021-1 et ISO 19011.

Le processus de certification implique l'audit du *système* de *gestion* pour le respect de la norme ISO / CEI 27001. Les auditeurs de certification n'ont qu'un intérêt passager pour les risques d'information réels et les contrôles de sécurité gérés par le système de gestion. Il est supposé que toute organisation avec un SMSI conforme gère effectivement ses risques d'information avec diligence. [15]

Statut de la norme

L'ISO / CEI 27006 a été publiée pour la première fois en 2007. Elle a incorporé et remplacé les anciennes directives sur les processus de certification accrédités.

Une fois l'ISO 17021 révisé, une mise à jour rapide a été réalisée et une deuxième édition légèrement révisée de l'ISO / CEI 27006 a été publiée en 2011. La norme a ensuite été examinée parallèlement à la révision de l'ISO 19011 et de l'ISO / CEI 17021, Suite à la publication de la version 2013 de la norme ISO / CEI 27001.

8) L'ISO/CEI 27007

L'ISO / CEI 27007 fournit des conseils aux organismes de certification accrédités, aux auditeurs internes, aux vérificateurs externes / tiers et à d'autres personnes qui vérifient les SMSI par rapport à la norme ISO / CEI 27001 (c'est-à-dire auditant le système de gestion pour se conformer à la norme).

L'ISO / CEI 27007 s'appuie fortement sur l'ISO 19011 , la norme pour les systèmes de gestion de l'audit, fournissant des conseils spécifiques à le SMSI.

La norme couvre les aspects spécifiques à l'ASSMS de la vérification de la conformité :

- Gérer le programme d'audit SMSI (déterminer ce qu'il faut auditer, quand et comment, affecter les auditeurs appropriés, gérer les risques d'audit, conserver les enregistrements d'audit, améliorer les processus continus) ;
- Effectuer une vérification (processus de vérification - planification, conduite, principales activités d'audit, y compris le travail sur le terrain, l'analyse, le rapport et le suivi) ;
- Gestion des auditeurs du SMSI (compétences, compétences, attributs, évaluation).

Le corps principal de la norme conseille principalement sur l'application de l'ISO 19011 au contexte du SMSI, avec quelques commentaires explicatifs pas terriblement utiles. Toutefois, l'annexe énonce plus en détail des tests d'audit spécifiques concernant la conformité de l'organisation avec le corps principal de l'ISO / CEI 27001 . [16]

Statut de la norme

La norme a été publiée en novembre 2011. L'ISO 19011 a également été révisé et publié en 2011. La norme est en cours en révision.

Conclusion :

Nous avons introduit dans ce chapitre la notion du standard et de référentiel faire une étude comparative entre eux, puis on a fait une étude détaillée sur la série des normes ISO/IEC 2700x on basant sur la norme ISO/IEC 27001 qui est le point de gravité de cette série.

D'où, le chapitre suivant est consacré à l'analyse et l'implémentation du SMSI conforme à cette série qu'on a étudiée.

Chapitre 3 :

Analyse et Implémentation de SMSI et Présentation des mesures de sécurité proposée

Ce chapitre est composé de deux parties. Dans la première partie on va présenter la méthode EBIOS et comment elle répond à toutes les exigences d'ISO 27001 et aide à la mise en œuvre d'un SMSI au sein d'UNIDEES. Dans la deuxième partie on va présenter nos solutions pour couvrir les mesures de sécurité qui manquent par rapport au bonnes pratiques de ISO/IEC 27002.

Partie 1 : Analyse et Implémentation de SMSI

La mise en œuvre d'un SMSI conforme aux exigences d'ISO/IEC 27001 dans l'entreprise est un requis important pour la poursuite de ses activités et un garant de l'amélioration continue de la sécurité de ses informations, mais la réalisation de ce projet est compliqué, c'est pourquoi il existe des méthodes reconnues pour aider les responsables informatiques pour le réaliser.

Cette partie a pour but de présenter une étude comparative entre deux méthodes d'analyse des risques, elles sont conforme aux normes d'ISO 27001,27002et 27005, et elles sont les plus connus et les plus utiliser pour la mettre en œuvre d'un SMSI et organiser la sécurité aux sein des entreprises (EBIOS, MEHARI).

Etude comparative entre les méthodes d'analyse des risques :

1. La méthode EBIOS :

EBIOS est l'acronyme de « Expression des Besoins et Identification des Objectifs de Sécurité ». C'est une méthode publiée par la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) en France en 1995. [18]

La méthode EBIOS formalise une démarche de gestion des risques découpée en cinq modules représentés sur la figure suivante :

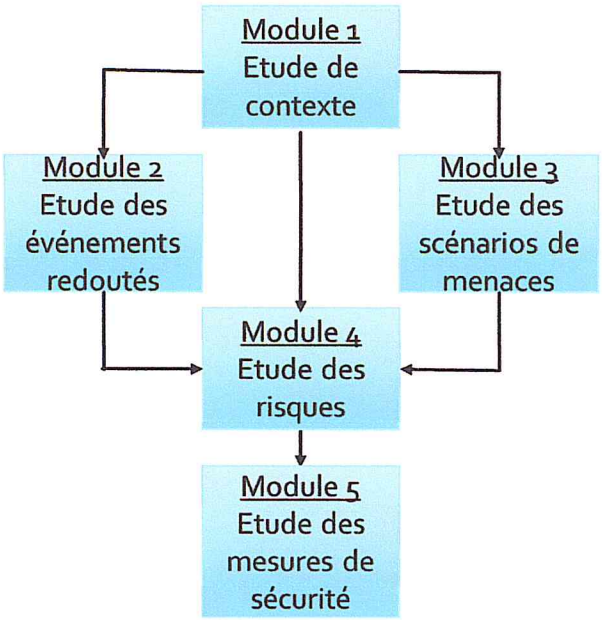


Figure 12 Diagramme montre les cinq modules de la méthode EBIOS

La démarche est dite itérative. En effet, il sera faite plusieurs fois appel à chaque module afin d'en améliorer progressivement le contenu, et la démarche globale sera également affinée et tenue à jour de manière continue.

Module 1 – Étude du contexte

À l'issue du premier module, qui s'inscrit dans l'établissement du contexte, le cadre de la gestion des risques, les métriques et le périmètre de l'étude sont parfaitement connus ; les biens essentiels, les biens supports sur lesquels ils reposent et les paramètres à prendre en compte dans le traitement des risques sont identifiés.

Module 2 – Étude des événements redoutés

Le second module contribue à l'appréciation des risques. Il permet d'identifier et d'estimer les besoins de sécurité des biens essentiels (en termes de disponibilité, d'intégrité, de confidentialité…), ainsi que tous les impacts (sur les missions, sur la sécurité des personnes, financiers, juridiques, sur l'image, sur l'environnement, sur les tiers et autres…) en cas de non-respect de ces besoins et les sources de menaces (humaines, environnementales, internes, externes, accidentelles, délibérées…) susceptibles d'en être à l'origine, ce qui permet de formuler les événements redoutés.

Module 3 – Étude des scénarios de menaces

Le troisième module s'inscrit aussi dans le cadre de l'appréciation des risques. Il consiste à identifier et estimer les scénarios qui peuvent engendrer les événements redoutés, et ainsi composer des risques. Pour ce faire, sont étudiées les menaces que les sources de menaces peuvent générer et les vulnérabilités exploitables.

Module 4 – Étude des risques

Le quatrième module met en évidence les risques pesant sur l'organisme en confrontant les événements redoutés aux scénarios de menaces. Il décrit également comment estimer et évaluer ces risques, et enfin comment identifier les objectifs de sécurité qu'il faudra atteindre pour les traiter.

Module 5 – Étude des mesures de sécurité

Le cinquième et dernier module s'inscrit dans le cadre du traitement des risques. Il explique comment spécifier les mesures de sécurité à mettre en œuvre, comment planifier la mise en œuvre de ces mesures et comment valider le traitement des risques et les risques résiduels.

Complexité de mise en œuvre :

La mise en œuvre de cette méthode est facilitée par la mise à disposition des utilisateurs de bases de connaissances riches et enrichissables, des guides méthodologiques gratuits permettant de simplifier l'application et la création des documents de synthèse. Par ailleurs, un club d'utilisateurs EBIOS a été créé en 2003 et constitue une communauté d'experts permettant le partage des expériences.

2. La méthode MEHARI :

MEHARI est l'acronyme de « Méthode Harmonisée d'Analyse des Risques ». Elle est développée et maintenue depuis 1995 par le CLUSIF (Club de la Sécurité de l'Information Français), reprend et remplace les méthodes MELISA et MARION. [19]

La méthode MEHARI formalise une démarche de gestion des risques découpée en trois grandes phases représentés sur la figure suivante :

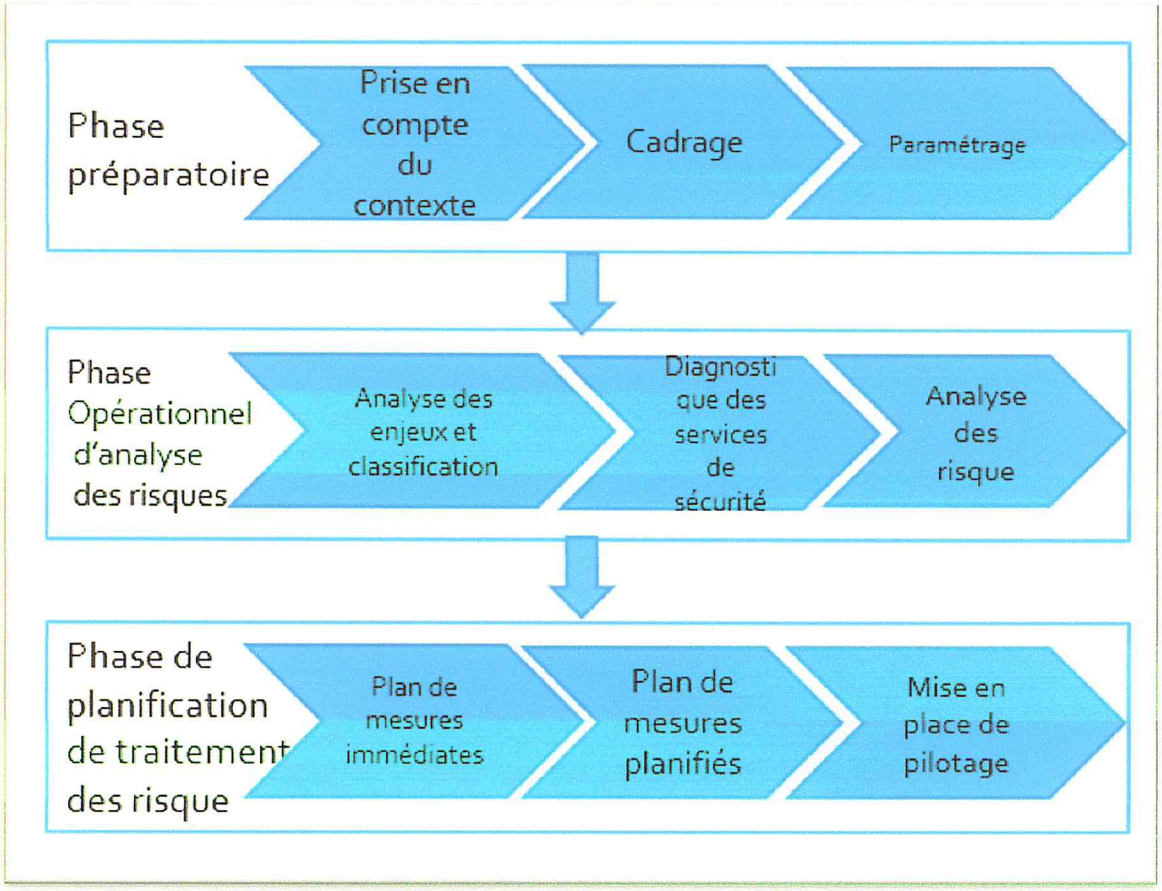


Figure 13 Diagramme montre les trois phases de la méthode MEHARI

La description de chaque phase de la méthode MEHARI :

La phase préparatoire :

Cette phase consiste à étudier le contexte et le périmètre de l'étude. Il s'agit d'identifier les événements pouvant impacter le fonctionnement du SI et d'évaluer la gravité de cet impact pour l'organisation. Il s'agit également de recenser et de classifier l'ensemble des actifs du SI. Cette phase permet de générer le Plan Stratégique de Sécurité (PSS). Le PSS fixe les objectifs de sécurité, c'est-à-dire le niveau de sécurité requis en termes de confidentialité, d'intégrité et de disponibilité pour chaque actif identifié. Il fixe également les métriques permettant d'évaluer le niveau de gravité d'un risque. Il définit la politique de sécurité ainsi que la charte d'utilisation du SI pour ses utilisateurs.

La phase opérationnelle d'analyse des risques :

Cette phase permet d'identifier les situations susceptibles de remettre en cause un des objectifs de sécurité de l'entreprise.
Il s'agit d'élaborer des scénarios de risque et d'effectuer un diagnostic des services de sécurité. Une évaluation des risques (probabilité, impact) est réalisée, permettant par la suite d'exprimer les besoins de sécurité, et les mesures nécessaires au traitement du risque.
Cette phase permet de générer le Plan Opérationnel de Sécurité (POS) qui définit les mesures de sécurité qui doivent être mises en œuvre.

La phase de planification du traitement des risques :

Cette phase consiste à analyser les scénarios de risque identifiés afin de décider du traitement à adopter :
• accepter le risque tel quel,
• réduire le risque, c'est-à-dire prendre des mesures pour réduire l'impact ou la potentialité du risque,
• éviter le risque, c'est-à-dire supprimer l'origine du risque par des mesures structurelles ou organisationnelles,
• transférer le risque, essentiellement par l'assurance.

Complexité de mise en œuvre :

La mise en œuvre de MEHARI ne peut être conduite qu'en conjonction avec des feuilles de calculs dédiés. Le démarrage de l'analyse nécessite une adaptation un peu compliquée de "la base de connaissances".

Les critères de choix :

Critères de choix d'une méthode d'analyse des risques :

- l'origine géographique de la méthode, la culture du pays jouant beaucoup sur le fonctionnement interne des entreprises et leur rapport au risque
- la langue de la méthode, il est essentiel de maîtriser le vocabulaire employé
- l'existence d'un club d'utilisateurs afin d'avoir un retour d'expériences
- la qualité de la documentation

- la facilité d'utilisation et le pragmatisme de la méthode
- la compatibilité avec une norme nationale ou internationale
- la quantité de moyens humains qu'elle implique et la durée de mobilisation
- la taille de l'entreprise à laquelle elle est adaptée
- sa popularité, une méthode très connue offre un réservoir de personnels qualifiés pour la mettre en œuvre

Choix important :

Selon les informations précédentes et les critères de choix, on a choisi la méthode EBIOS pour effectuer l'analyse des risques sur l'entreprise UNIDEES.

Et pour effectuer cette analyse on a choisi d'utiliser le Guide Méthodologique EBIOS crée par L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI Française) destinée au secteur public et au secteur privé, à des petites structures (petites et moyennes entreprises, collectivités territoriales…) et à des grandes structures (ministère, organisation internationale, entreprise multinationale…), à des systèmes en cours d'élaboration et à des systèmes existants.

Description de la démarche :

Avant de commencer la démarche de gestion des risques on a montré comment EBIOS a satisfait les exigences des normes ISO/IEC 27001 et ISO/IEC 27005. [18]

EBIOS satisfait les exigences de ISO/IEC 27001 :

Exigences de l' [ISO 27001] relatives à la gestion des risques	Activités d'EBIOS permettant de les satisfaire
4. Détermination de la portée du système de gestion de la sécurité de l'information : Lors de la détermination de cette portée, l'organisation doit tenir compte : • Les questions externes et internes visées à l'article 4.1. • Les exigences visées au point 4.2. • Les interfaces et les dépendances entre les activités réalisées par l'organisation et celles qui sont d'autres organisations.	Activité 1.1 – Définir le cadre de la gestion des risques Activité 1.3 – Identifier les biens

5.2 Politique : • Convient à l'objet de l'organisation. • Inclut des objectifs de sécurité de l'information (voir 6.2) ou fournit le cadre pour objectifs de sécurité. • S'engage à respecter les exigences applicables en matière de sécurité de l'information. • S'engage à améliorer continuellement le système de gestion de la sécurité de l'information. • Être disponibles en tant qu'informations documentées. • Être communiqués au sein de l'organisation. • Être à la disposition des parties intéressées, selon le cas.	Activité 1.1 – Définir le cadre de la gestion des risques Activité 1.2 – Préparer les métriques
6. Planification : 6.1 Généralités : Lors de la planification du système de gestion de la sécurité de l'information, l'organisation doit considérer les questions visées au point 4.1 et les exigences visées au point 4.2 et déterminer les risques et les possibilités Qui doivent être adressées à : ✓ Veiller à ce que le système de gestion de la sécurité de l'information puisse atteindre les résultats escomptés. ✓ Prévenir ou réduire les effets indésirables. ✓ Obtenir une amélioration continue. ✓ L'organisation doit faire des mesures visant à faire face à ces risques et à ces possibilités. ✓ Intégrer et mettre en œuvre les actions dans son système de gestion de la sécurité de l'information ✓ Évaluer l'efficacité de ces actions.	Activité 1.1 – Définir le cadre de la gestion des risques Activité 1.2 – Préparer les métriques
6.1.1 Évaluation des risques liés à la sécurité de l'information : • L'organisation doit définir et appliquer	

un processus d'évaluation des risques liés à la sécurité de l'information qui : ✓ Établit et maintenir des critères de risque de sécurité de l'information qui comprennent : ✓ Les critères d'acceptation des risques. ✓ Les critères d'évaluation des risques liés à la sécurité de l'information. ✓ Veillez à ce que les évaluations répétées des risques liés à la sécurité de l'information produisent des résultats comparables. • Identifie les risques liés à la sécurité de l'information : ✓ Appliquer le processus d'évaluation des risques liés à la sécurité de l'information afin d'identifier les risques associés à la perte de la Confidentialité, l'intégrité et la disponibilité des informations dans le cadre de l'information du Système de gestion de la sécurité. ✓ Identifier les propriétaires de risques (traçabilité). ✓ Évalue les risques liés à la sécurité de l'information : ✓ Comparer les résultats de l'analyse de risque avec les critères de risque. ✓ Prioriser les risques analysés pour le traitement du risque.	Activité 1.3 – Identifier les biens Activité 2.1 – Apprécier les événements redoutés Activité 3.1 – Apprécier les scénarios de menaces Activité 4.1 – Apprécier les risques
6.1.2 Traitement des risques liés à la sécurité de l'information : L'organisation doit définir et appliquer un processus de traitement des risques liés à la sécurité de l'information pour : ✓ Choisir des options appropriées de traitement des risques de sécurité de l'information, on considère les résultats d'évaluation. ✓ Déterminer tous les contrôles nécessaires à la mise en œuvre du traitement des risques liés à la sécurité de l'information. ✓ Comparer les contrôles déterminés avec ceux de l'annexe A et vérifier qu'aucun contrôle n'a été supprimée. ✓ Produire une déclaration d'applicatif contenant les contrôles nécessaires, Justification des inclusions (qu'elles soient mises en œuvre ou non),	Activité 2.1 – Apprécier les événements redoutés Activité 4.1 – Apprécier les risques

justification des exclusions des contrôles de l'annexe A. ✓ Formuler un plan de traitement des risques liés à la sécurité de l'information. ✓ Obtenir l'approbation du plan de traitement des risques liés à la sécurité de l'information et l'acceptation des risques résiduels de sécurité de l'information.	
6.2 Objectifs de sécurité de l'information et planification pour les atteindre : L'organisation doit établir des objectifs de sécurité de l'information aux fonctions et niveaux pertinents. Les objectifs de sécurité de l'information doivent : • Être conformes à la politique de sécurité de l'information. • Être mesurables (si possible). • Tenir compte des exigences de sécurité de l'information applicables et des résultats de l'évaluation des risques. • Le traitement des risques doit être communiqué et mis à jour le cas échéant. • L'organisation doit conserver des informations documentées sur les objectifs de sécurité de l'information lorsqu'elle planifie comment atteindre ses objectifs de sécurité de l'information, l'organisation doit déterminer : ✓ Ce qui sera fait. ✓ Quelles ressources seront nécessaires. ✓ Qui sera responsable. ✓ Quand il sera achevé. ✓ Comment les résultats seront évalués.	Activité 4.2 – Identifier les objectifs de sécurité
7.5 Exigences relatives à la documentation	Les données produites par les activités d'EBIOS permettent d'élaborer la plupart des documents exigés.
8. Fonctionnement : 8.1 Planification et contrôle opérationnels : • L'organisation doit planifier, mettre en œuvre et contrôler les processus nécessaires pour assurer la sécurité de l'information et de mettre en œuvre les	

actions définies au point 6.1. • L'organisation met également en objectifs de sécurité de l'information définis au point 6.2. • L'organisation doit conserver les informations documentées dans la mesure nécessaire pour avoir la certitude que les processus ont été exécutés comme prévu. • L'organisation doit contrôler les changements planifiés et examiner les conséquences des changements involontaires, Prendre des mesures pour atténuer les effets néfastes, si nécessaire. • L'organisation veille à ce que les processus impartis soient déterminés et contrôlés.	Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre
8.2 Évaluation des risques liés à la sécurité de l'information : • L'organisation doit effectuer des évaluations du risque de sécurité de l'information à des intervalles des changements importants sont proposés ou se produisent, en tenant compte des critères établis en 6.1.2 a). • L'organisation doit conserver des informations documentées sur les résultats de l'évaluation des risques.	Toutes les activités
8.3 Traitement des risques liés à la sécurité de l'information : • L'organisation met en œuvre le plan de traitement des risques liés à la sécurité de l'information. • L'organisation doit conserver des informations documentées sur les résultats du Risque.	Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre Activité 5.2 – Mettre en œuvre les mesures de sécurit
9. Évaluation du rendement : 9.1 Suivi, mesure, analyse et évaluation : • L'organisation doit évaluer la performance en matière de sécurité de l'information et l'efficacité système de	Toutes les activités

gestion de la sécurité de l'information. L'organisme doit déterminer : • Ce qui doit être surveillé et mesuré, y compris les processus et les contrôles de sécurité de l'information. • Les méthodes de surveillance, de mesure, d'analyse et d'évaluation, le cas échéant, pour des résultats valables. • Lorsque la surveillance et la mesure doivent être effectuées qui surveille et mesure ; • Lorsque les résultats de la surveillance et de la mesure doivent être analysés et évalués, analysera et évaluera ces résultats. • L'organisation doit conserver des informations documentées appropriées comme preuve des résultats de mesure. 9.2 Audit interne : L'organisation procède à des vérifications internes à intervalles prévus pour fournir des informations sur le système de gestion de la sécurité	
9.3 Examen de la gestion : La haute direction examine le système de gestion de la sécurité de l'information afin de s'assurer de son adéquation et de son efficacité.	Toutes les activités

Tableau 9 EBIOS satisfait les exigences de ISO/IEC 27001

EBIOS décline parfaitement l'ISO 27005 :

Chapitres de l'ISO 27005	Activités d'EBIOS correspondantes
7. Etablissement de contexte	Module 1 – Étude du contexte
7.1. Considérations générales	Module 1 – Étude du contexte
7.2. Critères de base	Activité 1.2 – Préparer les métriques
7.3. Portée et limites	Activité 1.3 – Identifier les biens
7.4. Organisation pour la gestion du risque de sécurité de l'information	Activité 1.1 – Définir le cadre de la gestion des risques
8. Évaluation des risques liés à la sécurité de l'information	Module 2 – Étude des événements redoutés Module 3 – Étude des scénarios de menaces Module 4 – Étude des risques
8.1. Description générale de l'évaluation du risque de sécurité de l'information	Module 2 – Étude des événements redoutés Module 3 – Étude des scénarios de menaces Module 4 – Étude des risques
8.2. Identification des risques	Module 2 – Étude des événements redoutés

	Module 3 – Étude des scénarios de menaces Module 4 – Étude des risques
8.3. Analyse de risque	Module 4 – Étude des risques
9. Traitement des risques pour la sécurité de l'information	Module 4 – Étude des risques Module 5 – Étude des mesures de sécurité
9.1. Description générale du traitement des risques	Module 4 – Étude des risques Module 5 – Étude des mesures de sécurité
9.2. Modification des risques	Activité 4.2 – Identifier les objectifs de sécurité Module 5 – Étude des mesures de sécurité
9.3. Retenue de risque	Activité 4.2 – Identifier les objectifs de sécurité Module 5 – Étude des mesures de sécurité
9.4. Évitement des risques	Activité 4.2 – Identifier les objectifs de sécurité Module 5 – Étude des mesures de sécurité
9.5. Partage des risques	Activité 4.2 – Identifier les objectifs de sécurité Module 5 – Étude des mesures de sécurité
10. Acceptation du risque de sécurité de l'information	Activité 5.2 – Mettre en œuvre les mesures de sécurité
11. Communication et consultation sur les risques pour la sécurité de l'information	Toutes les activités (partie Communication et concertation)
12. Suivi et examen des risques liés à la sécurité de l'information	Toutes les activités (partie Surveillance et revue)
12.1. Suivi et évaluation des facteurs de risque	Toutes les activités (partie Surveillance et revue)
12.2. Surveillance, examen et amélioration de la gestion des risques	Toutes les activités (partie Surveillance et revue)

Tableau 10 EBIOS satisfait les exigences de ISO/IEC 27005

1. Module 1 – Étude du contexte :

Activité 1.1 – Définir le cadre de la gestion des risques

Objectif

Cette activité fait partie de l'établissement du contexte. Elle a pour but de circonscrire le périmètre d'étude et de définir le cadre dans lequel la gestion des risques va être réalisée.

Action 1.1.1. Cadrer l'étude des risques :

L'objectif de l'étude :

- ✓ Mettre en place un système de management de la sécurité de l'information.
- ✓ Gérer les risques SSI sur le long terme.

✓ Elaborer une politique de sécurité de l'information qui doit ainsi être produite, appliquée et contrôlée.

La structure de travail : (matrice RACI)

Activités d'EBIOS	Directeur	Comité de suivi (responsable informatique et Analyste de la sécurité de l'information)	Ingénieurs de sécurité des SI stagiaires	Service commercial et service administratif	Documents à produire en plus de l'étude des risques	Consignes particulières	Ressources estimées (en h.j)	Durée (en jours)
1.1 – Définir le cadre de la gestion des risques		C	R	I			3	4
1.2 – Préparer les métriques		C	R	I			3	4
1.3 – Identifier les biens	A	C	R	C		Ne pas trop détailler	6	4
2.1 – Apprécier les événements redoutés		C	R	C		Utiliser les bases génériques	6	4
3.1 – Apprécier les scénarios de menaces		C	R	C		Utiliser les bases génériques	6	4
4.1 – Apprécier les risques		C	R	I			3	2
4.2 – Identifier les objectifs de sécurité	A	C	R	I	-Note de stratégie		3	2
5.1 – Formaliser les mesures de sécurité à mettre en œuvre	A	C	R	C	-Politique de sécurité de l'information -Déclaration d'applicabilité		9	6

5.2 – Mettre en œuvre les mesures de sécurité	A	I	R	C			-	-

Figure 14 Matrice RACI montre les différents rôles et responsabilités lié à cette étude

Action 1.1.2. Décrire le contexte général :

Présentation de l'organisation et leurs principales missions :

UNIDEES Algérie, entreprise spécialisée dans le conseil, l'intégration et l'infogérance en sécurité des systèmes d'information, évolue dans des environnements où l'exigence est permanente (Energie, Industries, Défense, Télécom…).

Chaque jour, les collaborateurs d'UNIDEES Algérie contribuent au développement et à la performance des entreprises.

Leurs clients ont des métiers différents, mais ils partagent un même besoin, de fiabilité, de qualité, de rigueur, d'innovation et de sécurité quand il s'agit de gérer leurs systèmes sensibles.

Les métiers principaux qu'UNIDEES Algérie représentés sont la sécurité des systèmes d'informations et l'architecture des réseaux.

Sa structure organisationnelle est fonctionnelle avec 3 directions (administrative, commerciale, technique).

- Direction administrative : gère les ressources humaines et la comptabilité.

  Cette direction a l'accès au serveur des fichiers via l'application CRM (une application métier crée en PHP).

- Direction commerciale : gère les clients.

  Cette direction gère les clients via l'application métier qui s'appelle CRM pour gère leur clients et aussi elle permet l'accès au serveur des fichiers.

- Direction technique : répondre aux besoins des clients (installer des équipements, faire des formations…) et gère la sécurité de l'entreprise.

Cette direction a une application métier qui s'appelle SUPPORT/TIQUETTE (une application web crée en PHP) pour contacter et résoudre les problèmes des clients.

SUPPORT/TIQUETTE : cette application n'offre pas une interface client (elle reçoit les problèmes ou bien les demandes des clients sous forme d'un émail et de la même façon elle envoi les solutions et les réponses de service technique).

Les rôles et responsabilités en matière de gestion des risques sont les suivants :

Le Directeur d'UNIDEES est pleinement responsable des risques pesant sur sa société.

Les ingénieurs de sécurité stagiaires ont été choisi pour animer la gestion des risques de sécurité de l'information ils sont ainsi responsables de la réalisation des études de risques.

Un comité de suivi, composé d'un responsable informatique et un analyste de la sécurité de l'information, elle réalisera la première étude de risques et se réunira ensuite tous les six mois afin de faire le point sur les évolutions à apporter à la gestion des risques de sécurité de l'information.

Les interfaces de la gestion des risques sont les suivantes :

La gestion des risques de sécurité de l'information est partie intégrante de la gestion d'UNIDEES, à ce titre, ses résultats sont pris en compte dans la stratégie de la société.

L'ensemble de la société est concerné par la gestion des risques de sécurité de l'information, tant pour apprécier les risques que pour appliquer et faire appliquer des mesures de sécurité.

Action 1.1.3. Délimiter le périmètre de l'étude :

L'étude sera appliquée sur toute l'entreprise sans avoir besoin de la décomposer sur des sous-ensembles, par ce que l'entreprise a un seul réseau local et tous leurs départements sont situés dans le même bâtiment.

Les enjeux suivants ont été identifiés :

- Garantir la protection des informations sensibles des clients et employées.
- Garantir la protection de nos systèmes d'informations.

Les participants à l'étude sont définis comme suit :

Au moins un personnel de chaque direction (administrative, commerciale, technique) participe à l'étude.

D'autres personnels peuvent également participer à l'étude afin d'apporter un point de vue extérieur.

Les critères de sélection sont les meilleures connaissances du métier en général, et des processus d'UNIDEES.

Action 1.1.4. Identifier les paramètres à prendre en compte :

Un ensemble de contraintes à prendre en compte a été identifié :

Relatives au personnel :

- Le personnel de la direction commerciale et la direction administrative sont des utilisateurs de l'informatique, mais pas spécialiste.

D'ordre technique :

- Les applications métier doivent être employés ;

D'environnement :

- L'entreprise loue un immeuble complet au centre-ville,
- L'entreprise est au voisinage de commerces divers,
- Aucun déménagement n'est planifié.

Action 1.1.5. Identifier les sources de menaces :

Types de sources de menaces	Retenu ou non	Exemples
Source humaine interne, malveillante, avec de faibles capacités	Oui	• personnel en fin de contrat
Source humaine interne, malveillante, avec des capacités importantes	Oui	• manager ambitieux en fin de contrat
Source humaine interne, malveillante, avec des capacités illimitées	Oui	• administrateur système ou réseau agissant par vengeance
Source humaine externe, malveillante, avec de faibles capacités	Oui	• Script-kiddies. • Vandale.
Source humaine externe, malveillante, avec des capacités importantes	Oui	• Concurrent. • pirate passionné.
Source humaine externe, malveillante, avec des capacités illimitées	Oui	• espions.

Source humaine interne, sans intention de nuire, avec de faibles capacités	Oui	• stagiaire. • Utilisateur.
Source humaine interne, sans intention de nuire, avec des capacités importantes	Oui	• Manager. • développeur.
Source humaine interne, sans intention de nuire, avec des capacités illimitées	Oui	• administrateur système ou réseau.
Source humaine externe, sans intention de nuire, avec de faibles capacités	Oui	• personne réalisant des travaux dans le voisinage.
Source humaine externe, sans intention de nuire, avec des capacités importantes	Oui	• visiteur maladroit. • Fournisseur d'accès Internet. • Hébergeur.
Source humaine externe, sans intention de nuire, avec des capacités illimitées	Oui	• explosion dans le voisinage.
Code malveillant d'origine inconnue	Oui	• Virus informatique.
Phénomène naturel	Oui	• Phénomène météorologique ou climatique.
Catastrophe naturelle ou sanitaire	Oui	• Phénomène géologique.
Activité animale	Non.	
Événement interne	Oui	• incendie des locaux.

Tableau 11 Identification des sources de menaces

Activité 1.2 – Préparer les métriques :

Objectif

Cette activité fait partie de l'établissement du contexte. Elle a pour but de fixer l'ensemble des paramètres et des échelles qui serviront à gérer les risques. Elle peut être commune à plusieurs études.

Action 1.2.1. Définir les critères de sécurité et élaborer les échelles de besoins :

Cette action consiste à choisir les critères de sécurité qui seront étudiés, à produire une définition pour chacun d'eux et à élaborer autant d'échelles de besoins que de critères de sécurité retenus.

Les critères de sécurité constituent des facteurs permettant de relativiser l'importance des différents biens essentiels selon les besoins métiers, et serviront ainsi à décrire les conditions dans lesquelles le métier s'exerce convenablement.

Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Critères de sécurité	Définitions
Disponibilité	faculté d'un système à fonctionner dans des conditions

	prédéterminées d'exploitation et de maintenance (de délais et de performances).
Intégrité	consistant à empêcher les altérations, suppressions ou ajouts d'informations non autorisées.
Confidentialité	consistant à empêcher la divulgation d'informations à des personnes non autorisées.

Tableau 12 Les critères de sécurité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes des critères de sécurité retenue :

	Confidentialité	Disponibilité	Intégrité
Niveaux de l'échelle	Public	Aucun besoin de disponibilité	Aucun besoin d'intégrité
	Le bien est accessible à tous sans aucune restriction.	Le bien peut être indisponible définitivement ou pas, sans que cela ait une conséquence.	Le bien peut ne pas être intègre si l'altération est identifiée.
	Limité	Long terme	
	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.	Le bien peut être indisponible plus d'une semaine, mais il ne doit pas être perdu définitivement	
	Réservé	Moyen terme	Besoin d'intégrité moyen
	Le bien est accessible seulement aux collaborateurs du Groupe.	Le bien doit être disponible dans la semaine.	Besoin d'intégrité moyen
	Confidentiel	Court terme	
	Le bien est accessible seulement aux personnes du Groupe directement concernées par cet élément.	Le bien doit être disponible dans la journée.	
	Secret	Très court terme	Parfaitement intègre
	Le bien est très sensible, seules certaines personnes identifiées peuvent y accéder.	Le bien doit être disponible en temps réel.	Le bien doit être parfaitement intègre.

Tableau 13 les besoins de sécurité en termes des critères de sécurité

Action 1.2.2. Élaborer une échelle de niveaux de gravité :

Cette action consiste à créer une échelle décrivant tous les niveaux possibles des impacts. Tout comme les échelles de besoins, une échelle de niveaux d'impacts est généralement ordinale (les objets sont classés par ordre de grandeur, les nombres indiquent des rangs et non des quantités) et composée de plusieurs niveaux permettant de classer l'ensemble des risques. Chaque niveau reflète l'estimation de la hauteur des conséquences cumulées d'un sinistre

L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
Négligeable	surmontera les impacts sans aucune difficulté.
Limitée	surmontera les impacts malgré quelques difficultés.
Importante	surmontera les impacts avec de sérieuses difficultés.
Critique	ne surmontera pas les impacts.

Tableau 14 Description des niveaux de l'échelle (la gravité)

Action 1.2.3. Élaborer une échelle de niveaux de vraisemblance :

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
Minime	Cela ne devrait pas se (re)produire.
Significative	Cela pourrait se (re)produire.
Forte	Cela devrait se (re)produire un jour ou l'autre.
Maximale	Cela va certainement se (re)produire prochainement.

Tableau 15 Description des niveaux de l'échelle (la vraisemblance)

Action 1.2.4. Définir les critères de gestion des risques :

Action	Critère de gestion des risques (règle choisie pour réaliser l'action)
Estimation des événements redoutés et des scénarios de menaces	Les événements redoutés sont estimés en termes de gravité à l'aide de l'échelle définie à cet effet.
Évaluation des événements redoutés et des scénarios	• Les événements redoutés sont classés par ordre décroissant de vraisemblance.

de menaces	
Estimation des risques	• La gravité d'un risque est égale à celle de l'événement redouté considéré. • La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré.
Évaluation des risques	• Les risques dont la gravité est critique, et ceux dont la gravité est importante et la vraisemblance forte ou maximale, sont jugés comme dangereux. • Les risques dont la gravité est importante et la vraisemblance significative, et ceux dont la gravité est limitée et la vraisemblance forte ou maximale, sont jugés comme significatifs. • Les autres risques sont jugés comme négligeables.

Tableau 16 Critères de gestion des risques

Activité 1.3 – Identifier les biens :

Objectif

Cette activité fait partie de l'établissement du contexte. Elle a pour but d'identifier les biens au sein du périmètre de l'étude et ainsi de mettre en évidence les éléments nécessaires aux autres activités.

Action 1.3.1. Identifier les biens essentiels, leurs relations et leurs dépositaires :

Processus essentiels	Informations essentielles concernées	Dépositaires
La gestion des clients (cordonnées, contrats, facteurs…)	• CRM (App web) • Catalogues techniques. • Contrat. • Devis.	Direction commerciale.
La gestion des évènements et formations	• Fiche technique. • Liste des invités. • Supports de cours. • Contrat/Facteur.	Toutes les directions.
Gérer le site web	• Site web.	Direction technique.
Gérer la communication avec les clients via l'application SUPPORT	• Application web SUPPORT/TIQUETTE.	Direction technique.

Tableau 17 Processus essentiels

Action 1.3.2. Identifier les biens supports, leurs relations et leurs propriétaires :

Les types de biens supports représentent les grandes catégories de composants d'un système d'information sur lesquels reposent les biens essentiels et/ou les mesures de sécurité.

Note : Dans cette étape on a choisi de ne pas détailler chaque bien support appart mais de procéder par catégorie.

Les biens supports sont :

- ✓ Les systèmes informatiques et de téléphonie (SYS), qui peuvent être décomposés en matériels (MAT), logiciels (LOG), canaux informatiques et de téléphonie (RSX).
- ✓ Les organisations (ORG), qui peuvent être décomposées en personnes (PER), supports papier (PAP) et les canaux interpersonnels (CAN).
- ✓ Les locaux (LOC) : qui hébergent les autres biens supports et fournissent les ressources.

Note 1: les solutions de sécurité (procédures, produits…) ne sont pas considérées comme des biens supports ; elles sont en effet prises en compte en cours d'étude dans les "mesures de sécurité existantes" ou à la fin de l'étude dans les "mesures de sécurité" destinées à traiter les risques.

Note 2 : dans cette étape on a choisi de ne pas détailler chaque support appart mais on le prendre avec catégorie.

En interne :

- SYS – Réseau interne.

MAT-ENSEMBLE : (Ordinateur/Serveur, Périphérique informatique, Relais de communication, Support électronique).

MAT : (MAT serveur, MAT serveur web, MAT WIFI, MAT switch, MAT PC portable, MAT PC bureau, MAT IPBX, MAT téléphone fixe, MAT téléphone portable, MAT FAX, MAT imprimant, MAT disque dure externe…)

LOG-ENSEMBLE : (Application, Système de gestion de base de données, Système d'exploitation).

RSX-ENSEMBLE : (Canal informatique, Canal de téléphonie analogique).

- ORG – Organisation de l'entreprise.

PER – Personnes

PAP – Supports papier

CAN – Canaux interpersonnels

- LOC – Locaux de l'entreprise.

Un seul bâtiment.

En externe :

- SYS – Système de l'hébergeur (Internet et par courrier électronique).
- ORG – Hébergeur (par courrier papier).
- SYS – Internet (pour des accès distants et le courrier électronique).
- ORG – Partenaire (partenaire d'UNIDEES, clients…).

Action 1.3.3. Déterminer le lien entre les biens essentiels et les biens supports :

Biens supports	La gestion des clients (cordonnées, contrats, facteurs…)	La gestion des évènements et formations	Gérer le site web	Gérer la communication avec les clients via l'application SUPPORT
SYS – Réseau interne.	×		×	×
• MAT-ENSEMBLE	×		×	×
• LOG-ENSEMBLE	×		×	×
• RSX-ENSEMBLE	×		×	×
ORG – Organisation du l'entreprise	×	×	×	×
• PER – Personnes INTERNE	×	×	×	×
• PAP – Supports papier	×	×	×	×
• CAN – Canaux interpersonnels	×	×	×	×

SYS - Réseau EXTERNE-INTERNET			×	×
• MAT-ENSEMBLE-EX			×	×
• LOG-ENSEMBLE-EX			×	×
• RSX-ENSEMBLE-EX			×	×
• PER – Personnes CLIENTS			×	×
SYS – Système de l'hébergeur			×	×
ORG – Hébergeur			×	×
ORG – Partenaire	×	×	×	×

Tableau 18 le lien entre les biens essentiels et les biens supports

Action 1.3.4. Identifier les mesures de sécurité existantes :

Mesure de sécurité	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Tous les rôles et responsabilités en matière de sécurité de l'information sont définis et attribuées au responsable informatique qui occupe la répartition des tâches selon les profiles des employées.	ORG – Organisation du l'entreprise	6.1.1 Rôles et responsabilités en matière de sécurité de l'information. 6.1.2 La répartition des tâches.	×	×	
La solution Kaspersky crypté les données des pc portables de travail qui garantit la non divulgation des informations confidentiels le cas de vol de l'appareil.	MAT-ENSEMBLE	6.2.1 Politique de l'appareil mobile	×	×	

Tous les procédures et conditions d'emploi sont définie et gérer par le service des ressources humains.	ORG – Organisation du l'entreprise	7.1.1 Dépistage	×		
La procédure disciplinaire est définie et gérer par le service des ressources humains.	ORG – Organisation du l'entreprise	7.2.3 Procédé de discipline	×		
La procédure de résiliation et changement d'emploi est définie et gérer par le service des ressources humains et le responsable informatique.	ORG – Organisation du l'entreprise	7.3 Résiliation et changement d'emploi	×		
La procédure de cessation est définie et gérer par le service des ressources humains et le responsable informatique.	ORG – Organisation du l'entreprise	7.3.1 Cessation ou du changement des responsabilités de l'emploi	×		
Classification des informations d'UNIDEES	ORG – Organisation du l'entreprise	8.2.1 Classification de l'information	×	×	
Création des lignes directrices pour protéger les médias contenant des informations transportées (transport fiable, l'emballage, lister les courriers autorisées…).	ORG – Organisation du l'entreprise	8.3.3 Transfert physique des médias	×	×	×
La politique d'accès et les outils technique comme PAR-FEU, SSO-WALLIX, AD	ORG – Organisation du l'entreprise	9. contrôle d'accès	×		
Solution Kaspersky	MAT-ENSEMBLE	10. Cryptographie	×	×	
Installer des caméras de surveillance et des agents 24/7	ORG – Organisation du l'entreprise	11.1 Zones sécurisées	×		
Contrôler l'installation et l'utilisation des équipements. Climatisation.	ORG – Organisation du l'entreprise	11.2 Équipement	×	×	

Procédure de changement de système (faire une gestion des risques avant de commencer le projet, obtenir l'approbation de la direction…). Serveur Test. Hors les heurs d'emploi. Documenté tous les changements. Back up.	ORG – Organisation du l'entreprise	12.1.2 Gestion du changement 14.2.2 Procédures de contrôle de changement du système 14.2.3 Examen technique des applications après les modifications de la plate-forme d'exploitation 14.2.4 Restrictions sur les modifications aux logiciels	×	×	×
La capacité de stockage des serveurs d'UNIDEES et la virtualisation.	ORG – Organisation du l'entreprise MAT-ENSEMBLE	12.1.3 Gestion des capacités	×	×	
Serveur Test séparé aux autres serveurs et privilège de Windows	MAT-ENSEMBLE ORG – Organisation du l'entreprise	12.1.4 Séparation du développement, des tests et des environnements opérationnels	×	×	
Kaspersky, session de Windows.	MAT-ENSEMBLE ORG – Organisation du l'entreprise	12.2.1 Contrôles contre les logiciels malveillants	×	×	
Wallix et ID	MAT-ENSEMBLE	12.4.1 Enregistrement des événements		×	×
Authentification	ORG – Organisation du l'entreprise	12.4.2 Protection des informations du journal		×	
UTC+ 01 : 00	ORG – Organisation du l'entreprise	12.4.4 Synchronisation d'horloge	×	×	×
Kaspersky, session de Windows	MAT-ENSEMBLE ORG – Organisation du l'entreprise	12.5.1 Installation de logiciels sur les systèmes d'exploitation	×	×	
Kaspersky et WAF	MAT-ENSEMBLE	12.6.1 Gestion des vulnérabilités techniques	×	×	×
Kaspersky et Authentification	MAT-ENSEMBLE	12.6.2 Restrictions sur l'installation du logiciel	×	×	

Les tests et les maintenances se font généralement hors les heures de travail	ORG – Organisation du l'entreprise	12.7.1 contrôles et vérification des Systèmes d'information	×	×	
Pare-feu, logiciel de détection d'intrusion et le chiffrement(Kaspersky)	SYS-Réseau interne	13.1.2 Sécurité des services réseau	×	×	
Architecture de réseau sécurisée et authentification	SYS-Réseau interne	13.1.3 Ségrégation dans les réseaux	×	×	
Messagerie électronique	ORG – Hébergeur	13.2 Transfert d'information	×	×	×
Authentification, chiffrement et signatures	MAT-ENSEMBLE	14.1.3 Protéger les transactions de services d'application	×	×	×
Les compétences des employer d'UNIDEES garantie le suivi des règles défini dans ce contrôle	ORG – Organisation du l'entreprise	14.2.1 Politique de développement sécurisé	×	×	
Contrat avec services externalisés (site web, messagerie)	ORG – Hébergeur	14.2.5 Principes d'ingénierie du système sécurisé	×	×	×
Réaliser un test de système avant le mètre dans l'environnement de l'organisation	MAT Serveur-Test	14.2.7 Développement Outsourced 14.2.9 Tests d'acceptation du système	×	×	
Suppression de toutes informations confidentielles dans l'environnement de test après la fin de procédure de test	ORG – Organisation du l'entreprise	14.3.1 Protection des données de test	×	×	
Les fournisseurs doivent respecter les exigeasses de sécurité de l'entreprise.	ORG – Partenaire	15.1 Sécurité de l'information dans les relations avec les fournisseurs	×	×	×
UNIDEES a des procédures de contrôle et de suivi des services des fournisseurs	ORG – Organisation du l'entreprise	15.2 Gestion de la prestation des services de fournisseur	×	×	×
Analyste de la sécurité de l'information est responsable sur la gestion des incidents (manque de	ORG – Organisation du l'entreprise	16 gestions des incidents de sécurité de l'information	×	×	×

sensibilisations, procédure documenté de reprise après incident)					
Wallix et authentification ID	MAT-ENSEMBLE	16.1.7 Collection des preuves			×
Vérifier, examiner et évaluer la continuité de sécurité de l'information (le cas échéant Backup existe)	ORG – Organisation du l'entreprise	17.1 Continuité de sécurité de l'information	×	×	×
UNIDEES a un Pen testeur spécialisé pour faire la gestion des vulnérabilités	ORG – Organisation du l'entreprise	18.2.3 Examen de la conformité technique	×	×	

Tableau 19 Les mesures de sécurités existantes

2. Module 2 – Étude des événements redoutés :

Activité 2.1 – Apprécier les événements redoutés

Objectif

Cette activité fait partie de l'appréciation des risques. Elle a pour but de faire émerger et de caractériser les événements liés à la sécurité de l'information que l'organisme redoute, sans étudier la manière dont ceux-ci peuvent arriver. Elle permet également de fournir les éléments nécessaires au choix de traitement des risques afférents et à la définition des priorités de traitement.

Action 2.1.1. Analyser tous les événements redoutés :

Cette action consiste à identifier et à estimer les événements redoutés pour chaque critère de sécurité et chaque bien essentiel identifié. On va ainsi faire émerger les besoins de sécurité des biens essentiels, les impacts encourus au cas où ils ne seraient pas respectés et les sources de menaces susceptibles d'en être à l'origine, et leur attribuer un niveau de gravité.

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
La gestion des clients				
L'indisponibilité	Court terme	• Employé peu	• difficulté	Important

de service de gestion des clients		sérieux • Incendie des locaux • Panne électrique • Virus non ciblé • Personnel de nettoyage (soudoyé) • Problème de connexion réseau • Bug logiciel CRM	communiqué avec les clients • Perte d'un marché ou de clientèle • Perte de crédibilité. • Pert de productivité	
L'altération des informations des clients	Parfaitement intègre	• Employé peu sérieux • Virus non ciblé • vandale	• Impossibilité de signer un contrat • Perte d'un marché ou de clientèle • Impossibilité de remplir les obligations légales • Perte de crédibilité	Important
Accès non autorisé aux informations des clients	Confidentiel	• Employé peu sérieux • Virus non ciblé • Concurrent • Vandale • visiteur maladroit	• Perte d'un marché ou de clientèle • Action en justice à l'encontre du l'entreprise • Perte de crédibilité	Critique
La gestion des évènements et formations				
L'indisponibilité des documents de des évènements et des formations	Moyen terme	• Employé peu sérieux	• Perte d'un marché ou de clientèle	Négligeable
L'altération des documents des évènements et des formations	Besoin d'intégrité moyen	• Employé peu sérieux	• Perte d'un marché ou de clientèle	Limité
Le non confidentialité des documents des évènements et des formations	Limité	• Employé peu sérieux • visiteur maladroit	• Perte d'un marché ou de clientèle	Limité

Gérer le site web				
L'indisponibilité de site Web	Moyen terme	• Panne électrique • Virus non ciblé • Problème de connexion réseau • Script-kiddies • Hébergeur • Vandale	• Perte d'un marché ou de clientèle • Perte de crédibilité	Limité
Le non intégrité de site Web	Parfaitement intègre	• Virus non ciblé • Employé peu sérieux • Script-kiddies • Hébergeur • vandale	• Impossibilité de remplir les obligations légales • Perte de crédibilité • Action en justice à l'encontre du l'entreprise. • Perte de notoriété • Mise en danger (tous les systèmes de l'entreprise)	Important
Le non confidentialité de site Web	Public	-	-	Négligeable
Gérer la communication avec les clients via l'application SUPPORT				
L'indisponibilité de l'application SUPPORT	Court terme	• Panne électrique • Virus non ciblé • Problème de connexion réseau • Script-kiddies • Hébergeur • Vandale	• Perte d'un marché ou de clientèle • Perte de crédibilité	important
Le non intégrité de l'application SUPPORT	Parfaitement intègre	• Virus non ciblé • Employé peu sérieux • Script-kiddies • Hébergeur • vandale	• Impossibilité de remplir les obligations légales • Perte de crédibilité • Action en justice à l'encontre du	critique

			l'entreprise. • Perte de notoriété • Mise en danger (tous les systèmes de l'entreprise)	
Le non confidentialité de l'application SUPPORT	Secret	• Employé peu sérieux • Virus non ciblé • Script-kiddies • Hébergeur • Vandale	• remplir les obligations légales • Perte de crédibilité • Action en justice à l'encontre du la société • Perte de notoriété • Mise en danger (tous les systèmes de l'entreprise)	Critique

Tableau 20 Analyse des évènements redouté

Action 2.1.2. Évaluer chaque événement redouté :

Cette action consiste à juger de l'importance des événements redoutés en les hiérarchisant selon les critères de gestion des risques retenus.

Il convient essentiellement de fournir les éléments nécessaires pour décider de développer ou non l'étude concernant chaque événement redouté, de traiter ou non les risques afférents et de prioriser la mise en œuvre de leur traitement.

Gravité	Événements redoutés
Critique	• Accès non autorisé aux informations des clients • Le non intégrité de l'application SUPPORT • Le non confidentialité l'application SUPPORT
Important	• L'indisponibilité de service de gestion des clients • L'altération des informations des clients • L'indisponibilité de l'application SUPPORT • Le non intégrité de site Web
Limité	• L'altération des documents des évènements et des formations

	• Le non confidentialité des documents des évènements et des formations • L'indisponibilité de site Web
Négligeable	• L'indisponibilité des documents de des évènements et des formations • Le non confidentialité de site Web

Tableau 21 Evaluations des évènements redouté

3. Module 3 – Étude des scénarios de menaces :

Activité 3.1 – Apprécier les scénarios de menaces

Objectif

Cette activité fait partie de l'appréciation des risques. Elle a pour but d'identifier les différentes possibilités d'actions sur les biens supports, afin de disposer d'une liste complète de scénarios de menaces. Elle permet également de fournir les éléments nécessaires au choix de traitement des risques afférents et à la définition des priorités de traitement.

Action 3.1.1. Analyser tous les scénarios de menaces :

Cette action consiste à identifier les scénarios de menaces pour chaque critère de sécurité et chaque bien support identifié et à les estimer en termes de vraisemblance.

Les scénarios de menaces sont obtenus en questionnant les parties prenantes sur ce qu'elles savent et en approfondissant la réflexion jusqu'à ce que tous les éléments aient été formulés.

Scénarios de menaces	Sources de menaces	Vraisemblance
SYS – Réseau interne		
Menaces sur le réseau interne causant une indisponibilité	• Employé peu sérieux • Maintenance informatique • Script-kiddies • Virus non ciblé • Incendie des locaux • Panne électrique • Phénomène naturel (foudre, usure…)	Forte
Menaces sur le réseau interne causant une altération	• Employé peu sérieux • Maintenance informatique • Script-kiddies • Virus non ciblé	Maximale

Tableau 22 Analyse des scénarios de menace

Action 3.1.2. Évaluer chaque scénario de menace :

Cette action consiste à juger de l'importance des scénarios de menaces en les hiérarchisant selon les critères de gestion des risques retenus.

Il convient essentiellement de fournir les éléments nécessaires pour décider de traiter ou non les risques afférents et de prioriser la mise en œuvre de leur traitement.

Vraisemblance	Scénarios de menaces
Maximale	• Menaces sur le réseau interne causant une altération • Menaces sur le réseau interne causant une compromission • Menaces sur l'organisation causant une compromission • Menaces sur le système de l'hébergeur causant une indisponibilité • Menaces sur le système de l'hébergeur causant une compromission • Menaces sur un partenaire causant une compromission • Menaces sur Internet causant une indisponibilité
Forte	• Menaces sur le réseau interne causant une indisponibilité • Menaces sur le système de l'hébergeur causant une altération • Menaces sur un partenaire causant une indisponibilité • Menaces sur Internet causant une altération
Significative	• Menaces sur l'organisation causant une indisponibilité • Menaces sur l'hébergeur causant une indisponibilité • Menaces sur l'hébergeur causant une altération • Menaces sur Internet causant une compromission
Minime	• Menaces sur l'organisation causant une altération • Menaces sur l'hébergeur causant une compromission • Menaces sur un partenaire causant une altération

Tableau 23 Evaluation des scénarios de menace

4. Module 4 – Étude des risques :

Activité 4.1 – Apprécier les risques :

Objectif

Cette activité fait partie de l'appréciation des risques. Elle a pour but de mettre en évidence et de caractériser les risques réels pesant sur le périmètre de l'étude.

Action 4.1.1. Analyser les risques :

Cette action consiste à mettre en évidence l'ensemble des risques qui pèsent réellement sur le périmètre de l'étude et à déterminer leur gravité et leur vraisemblance, une première fois sans tenir compte des mesures de sécurité existantes, et une seconde fois en les prenant en compte. On fait ainsi le lien entre les événements redoutés et les scénarios de menaces, c'est-à-dire entre ce que l'organisme craint et ce à quoi il est exposé.

Risque	Gravité	Vraisemblance
Risque lié à l'indisponibilité de service de gestion des clients	Important	Forte
Risque lié à l'altération des informations des clients	Important	Maximale
Risque lié à l'accès non autorisé aux informations des clients	Critique	Maximale
Risque lié à l'indisponibilité des documents de des évènements et des formations	Négligeable	Significative
Risque lié à l'altération des documents des évènements et des formations	Limité	Minime
Risque lié au non confidentialité des documents des évènements et des formations	Limité	Maximale
Risque lié à l'indisponibilité de site Web	Limité	Maximale
Risque lié au non intégrité de site Web	Important	Maximale
Risque lié au non confidentialité de site Web	Négligeable	Maximale
Risque lié à l'indisponibilité de l'application SUPPORT	important	Maximale
Risque lié au non intégrité de l'application SUPPORT	critique	Maximale
Risque lié au non confidentialité de l'application SUPPORT	Critique	Maximale

Tableau 24 Analyse des risques

Niveau de risque après l'application des mesures de sécurité existantes :

- **Risque lié à l'indisponibilité de service de gestion des clients :**

On a établi la liste des risques à partir des événements redoutés et des scénarios de menaces précédemment appréciés. Les mesures de sécurité existantes ayant un effet sur chaque risque ont également été identifiées. La gravité et la vraisemblance ont finalement été estimées, sans, puis avec, les mesures de sécurité (les niveaux rayés correspondent aux valeurs avant application de ces mesures).

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
La gestion des clients				
L'indisponibilité de service de gestion des clients	Court terme	• Employé peu sérieux • Incendie des locaux • Panne électrique • Virus non ciblé • Personnel de nettoyage (soudoyé) • Problème de connexion réseau • Bug logiciel CRM	• difficulté communiqué avec les clients • Perte d'un marché ou de clientèle • Perte de crédibilité. • Pert de productivité	Important

Tableau 25 L'indisponibilité de service de gestion des clients

Scénarios de menaces	Sources de menaces	Vraisemblance
SYS – Réseau interne		
Menaces sur le réseau interne causant une indisponibilité	• Employé peu sérieux • Maintenance informatique • Script-kiddies • Virus non ciblé • Incendie des locaux • Panne électrique • Phénomène naturel (foudre, usure…)	Forte
ORG – Organisation du l'entreprise		
Menaces sur l'organisation causant une indisponibilité	• Employé peu sérieux • Personnel de nettoyage	Significative

Tableau 26 Scénarios de menaces sur le réseau interne et l'organisation de l'entreprise causent une indisponibilité.

Mesure de sécurité	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
La solution Kaspersky crypté les données des pc portables de travail qui garantit la non divulgation des informations confidentiels le cas de vol de l'appareil.	MAT-ENSEMBLE	6.2.1 Politique de l'appareil mobile	×	×	
La procédure disciplinaire est définie et gérer par le service des ressources humains.	ORG – Organisation du l'entreprise	7.2.3 Procédé de discipline			×
La politique d'accès et les outils technique comme PAR-FEU, SSO-WALLIX, AD	ORG – Organisation du l'entreprise	9. contrôle d'accès	×		
Solution Kaspersky	MAT-ENSEMBLE	10. Cryptographie	×	×	
Installer des caméras de surveillance et des agents 24/7	ORG – Organisation du l'entreprise	11.1 Zones sécurisées	×		
Contrôler l'installation et l'utilisation des équipements.	ORG – Organisation du l'entreprise	11.2 Équipement	×	×	
Procédure de changement de système (faire une gestion des risques avant de commencer le projet, obtenir l'approbation de la direction…). Serveur Test. Hors les heurs d'emploi. Documenté tous les changements. Back up.	ORG – Organisation du l'entreprise	12.1.2 Gestion du changement 14.2.2 Procédures de contrôle de changement du système 14.2.3 Examen technique des applications après les modifications de la plate-forme d'exploitation 14.2.4 Restrictions sur les modifications aux logiciels	×	×	×

La capacité de stockage des serveurs d'UNIDEES et la virtualisation.	ORG – Organisation du l'entreprise MAT-ENSEMBLE	12.1.3 Gestion des capacités	×	×	
Kaspersky, privilège de Windows.	MAT-ENSEMBLE	12.2.1 Contrôles contre les logiciels malveillants	×	×	
Authentification	ORG – Organisation du l'entreprise	12.4.2 Protection des informations du journal		×	
Kaspersky et Authentification	MAT-ENSEMBLE	12.6.2 Restrictions sur l'installation du logiciel	×	×	
Pare-feu, logiciel de détection d'intrusion et le chiffrement(Kaspersky)	SYS-Réseau interne	13.1.2 Sécurité des services réseau	×	×	
Wallix et authentification ID	MAT-ENSEMBLE	16.1.7 Collection des preuves			×

Tableau 27 mesures de sécurité pour modifier le risque 1

Niveau de risque				
Gravité	Négligeable	**Limitée**	~~**Importante**~~	Critique
Vraisemblance	Minime	**Significative**	~~**Forte**~~	Maximale

Tableau 28 Le résultat d'application des mesures de sécurité sur le risque 1

Note 1 : Pour chaque risque on doit évaluer la gravité de l'évènement redouter après l'application des mesures de sécurité protective et évaluer la vraisemblance des scénarios de menaces après l'application des mesure de sécurité préventive.

Note 2 : Tous les événements redoutés, scénarios de menaces et les mesures de sécurité existantes sont définit donc pour le reste des risques on a estimé la gravité et la vraisemblance en utilisant la même démarche et la tabla suivante vas présenter les résultats.

Résultats d'analyse des risques après l'application des mesures de sécurité existantes :

Risque	Gravité	Vraisemblance
Risque lié à l'indisponibilité de service de gestion des clients	~~Importante~~ Limité	~~Forte~~ Significative
Risque lié à l'altération des	Important	~~Maximale~~

informations des clients		Significative
Risque lié à l'accès non autorisé aux informations des clients	~~Critique~~ important	~~Maximale~~ Significative
Risque lié à l'indisponibilité des documents de des évènements et des formations	Négligeable	Significative
Risque lié à l'altération des documents des évènements et des formations	Limité	Minime
Risque lié au non confidentialité des documents des évènements et des formations	Limité	Maximal
Risque lié à l'indisponibilité de site Web	Limité	~~Maximale~~ Significative
Risque lié au non intégrité de site Web	Important	~~Maximale~~ Significative
Risque lié au non confidentialité de site Web	Négligeable	Maximale
Risque lié à l'indisponibilité de l'application SUPPORT	~~Important~~ Limité	Maximale
Risque lié au non intégrité de l'application SUPPORT	~~Critique~~ Important	Maximale
Risque lié au non confidentialité de l'application SUPPORT	~~Critique~~ Limité	Maximale

Les risques précédemment analysés (identifiés et estimés) peuvent être évalués à l'aide du tableau suivant :

Gravité	Critique				~~• Risque lié à l'accès non autorisé aux informations des clients~~ ~~• Risque lié au non intégrité de l'application SUPPORT~~ ~~• Risque lié au non confidentialité~~

					~~de l'application SUPPORT~~
	Importante		• Risque lié à l'altération des informations des clients • Risque lié à l'accès non autorisé aux informations des clients • Risque lié au non intégrité de site Web	• ~~Risque lié à l'indisponibilité de service de gestion des clients~~	• ~~Risque lié à l'altération des informations des clients~~ • ~~Risque lié au non intégrité de site Web~~ • ~~Risque lié à l'indisponibilité de l'application SUPPORT~~ • Risque lié au non intégrité de l'application SUPPORT
	Limité	• Risque lié à l'altération des documents des évènements et des formations	• Risque lié à l'indisponibilité de service de gestion des clients • Risque lié à l'indisponibilité de site Web		• Risque lié au non confidentialité des documents des évènements et des formations • ~~Risque lié à l'indisponibilité de site Web~~ • Risque lié à l'indisponibilité de l'application SUPPORT • Risque lié au non confidentialité de l'application SUPPORT
	Négligeable		• Risque lié à l'indisponibilité des documents de des évènements et des formations		• Risque lié au non confidentialité de site Web
Risques négligeables Risques significatifs Risques intolérables		Minime	Significative	Forte	Maximale
		Vraisemblance			

Tableau 29 Cartographier les risques

4.2 Identification des objectifs de sécurité

Les objectifs de sécurité : 8 risques à réduire en priorité

On souhaite essentiellement réduire les risques jugés comme prioritaires et significatifs, et prendre les risques jugés comme non prioritaires.

Le tableau suivant présente les objectifs de sécurité identifiés (les croix correspondent aux premiers choix) :

Risque	Evitement	Réduction	Prise	Transfert
Risque lié à l'indisponibilité de service de gestion des clients		×	×	
Risque lié à l'altération des informations des clients		×	×	
Risque lié à l'accès non autorisé aux informations des clients		×	×	
Risque lié à l'indisponibilité des documents de des évènements et des formations		×	×	
Risque lié à l'altération des documents des évènements et des formations		×	×	
Risque lié au non confidentialité des documents des évènements et des formations		×	×	
Risque lié à l'indisponibilité de site Web		×	×	
Risque lié au non intégrité de site Web		×	×	
Risque lié au non confidentialité de site Web		×	×	
Risque lié à l'indisponibilité de l'application SUPPORT		×	×	
Risque lié au non intégrité de l'application SUPPORT		×	×	
Risque lié au non confidentialité de l'application SUPPORT		×	×	

Tableau 30 Identification des objectifs de sécurité

Les risques résiduels : 4 risques jugés comme négligeables

À l'issue de l'identification des objectifs de sécurité, On a mis en évidence les risques résiduels suivants :

Risque	Gravité	Vraisemblance
Risque lié à l'indisponibilité des documents de des évènements et des formations	Négligeable	significative
Risque lié à l'altération des documents des évènements et des formations	Limité	Minime
Risque lié à l'indisponibilité de site Web	Limité	significative
Risque lié au non confidentialité de site Web	Négligeable	Maximale

Tableau 31 Les risques résiduels

On note que ces risques résiduels pourront être réduits ultérieurement, quand les autres risques seront devenus acceptables.

5. Module 5 – Étude des mesures de sécurité

Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre

Objectif

Cette activité fait partie du traitement des risques. Elle a pour but de déterminer les mesures de sécurité adéquates pour atteindre les objectifs de sécurité identifiés, d'identifier les risques résiduels et de valider "formellement" les choix effectués.

Mesures de sécurité complémentaires :

Le tableau suivant présente la liste des mesures de sécurité destinées à réduire les risques prioritaires (elles traitent également les autres risques) :

Mesure de sécurité (description)	Bien support sur lequel elle repose	Thème ISO 27002 (2013)	Prévention	Protection	Récupération
Un ensemble de politiques de sécurité de l'information devrait être défini, approuvé par la	ORG – Organisation du l'entreprise	5.1.1 Politiques pour la sécurité de l'information	×	×	×

direction, publié et Communiquées aux employés et aux parties externes pertinentes.					
Les politiques de sécurité de l'information devraient être revues à des intervalles planifiés ou si des changements importants se produisent pour assurer leur adéquation et leur efficacité.	ORG – Organisation du l'entreprise	5.1.2 Examen des politiques de sécurité de l'information	×	×	×
Sécurité de l'information devrait être traitée dans la gestion de projet, quel que soit le type de projet.	ORG – Organisation du l'entreprise	Sécurité de l'information dans la gestion de projet	×	×	×
La gestion devrait exiger que tous les employés et les entrepreneurs d'appliquer la sécurité de l'information selon les politiques et procédures établies de l'organisation.	ORG – Organisation du l'entreprise	7.2.1 Responsabilités de la direction	×	×	×
Tous les employés de l'organisation et les entrepreneurs concernés, devraient recevoir la sensibilisation appropriée éducation et de formation et des mises à jour régulières dans les politiques et procédures organisationnelles, comme pertinentes pour leur fonction.	ORG – Organisation du l'entreprise	7.2.2 Sensibilisation à la sécurité de l'information, l'éducation et la formation	×	×	×
La nécessite d'établir et maintenir l'inventaire des actifs pour des raisons comme la sécurité et l'assurance	ORG – Organisation du l'entreprise	8.1.1 Inventaire des actifs	×	×	×
La nécessite d'attribué à chaque actif un propriétaire	ORG – Organisation du l'entreprise	8.1.2 La propriété des actifs	×	×	×

Règles relatives à l'utilisation des actifs ou de l'information dois être définit et documentée.	ORG – Organisation du l'entreprise	8.1.3 L'utilisation acceptable des actifs	×	×	×
Un ensemble approprié de procédures pour l'étiquetage de l'information devrait être élaboré et mis en œuvre conformément au système de classification de l'information adoptée par l'organisation.	ORG – Organisation du l'entreprise	8.2.2 Etiquetage des informations	×	×	×
Des procédures doivent être établies pour la manipulation, le traitement, le stockage et la communication d'informations conformément à son classement.	ORG – Organisation du l'entreprise	8.2.3 Traitement des actifs	×	×	×
Des procédures devraient être mises en œuvre pour la gestion des supports amovibles conformément au système de classification adopté par l'organisation.	ORG – Organisation du l'entreprise	8.3.1 Gestion des supports amovibles	×	×	×
Création des procédures formelles pour l'élimination sûre des médias.	ORG – Organisation du l'entreprise	8.3.2 Mise au rebout des médias	×	×	×
Une politique de bureau claire pour les documents et les supports de stockage amovibles et une politique d'écran claire pour les installations de traitement de l'information devraient être adoptées.	ORG – Organisation du l'entreprise	11.2.9 Bureau claire et politique écran clair	×	×	×
Documentée les procédures d'exploitations existent à UNIDEES	ORG – Organisation du l'entreprise	12.1.1 Les procédures d'exploitation	×	×	×
Alimentation secourue	ORG – Organisation du l'entreprise	11.2 Équipement	×	×	

Séparer l'emplacement de serveur AD secondaire	ORG – Organisation du l'entreprise	12.3.1 Sauvegarde des informations	×	×	×
Définir un responsable qui gère le réseau et tous leurs équipements.	ORG – Organisation du l'entreprise	13.1.1 contrôles réseau	×	×	×
Identification des exigences de la sécurité de l'information.	ORG – Organisation du l'entreprise	14.1.1 exigences de sécurité de l'information analyse et la spécification	×	×	×
Toute modification doit être testée et documenté avant les mettre en place.	ORG – Organisation du l'entreprise	14.2.4 Restrictions sur les modifications aux logiciels	×	×	×
Les employés et les entrepreneurs qui utilisent les systèmes et services d'information de l'organisation devraient être tenus de noter et signaler les faiblesses de sécurité de l'information observées ou suspectées dans des systèmes ou des services.	ORG – Organisation du l'entreprise	16.1.3 Rapports sur les renseignements des failles de sécurité	×	×	×
Des lignes directrices doivent être mises pour la gestion des dossiers (stockage, manipulation, élimination…)	ORG – Organisation du l'entreprise	18.1.3 Protection des dossiers	×	×	×
L'approche de l'organisation de la gestion de la sécurité de l'information et sa mise en œuvre devraient être examinés indépendamment à intervalles réguliers ou lorsque des changements importants se produisent.	ORG – Organisation du l'entreprise	18.2.1 Examen indépendant de la sécurité de l'information	×	×	×
Les gestionnaires devraient revoir régulièrement la conformité par rapport aux normes et la politique de	ORG – Organisation du l'entreprise	18.2.2 Le respect des politiques de sécurité et des normes	×	×	×

sécurité.					

Tableau 32 Les mesures de sécurité complémentaire

Note : Les mesures de sécurité manquant dans l'entreprise UNIDEES sont des mesures organisationnelles, donc la mise en œuvre de ces derniers vont garantir la modification des risques prioritaires et résiduelle à un niveau acceptable.

Activité 5.2 – Mettre en œuvre les mesures de sécurité

Objectif

Cette activité fait partie du traitement des risques. Elle a pour but d'élaborer et de suivre la réalisation du plan de traitement des risques par les mesures de sécurité afin de pouvoir prononcer l'homologation de sécurité.

Action 5.2.1. Élaborer le plan d'action et suivre la réalisation des mesures de sécurité

Le plan d'action d'UNIDEES, trié par terme, avancement et coût financier, est établi comme suit :

Mesure de sécurité	Support	cout	Avancement
Etablir une politique de sécurité	document	-	Première version (terminer)
• Sensibilisation. • Communication. • L'inventaire des actifs. • Gestion des incidents. • Documenter les responsabilités en matière de sécurité de l'information. • Aider à réaliser un bon projet de gestion des risques à l'aide de messagerie, publications (statuts) et la participation de tous les employés. • Suivi la conformité de l'entreprise à l'aide d'un outil de communications et sensibilisation.	Application Web UNICOM	-	Au projet
Alimentation secourue	-	-	-

Tableau 33 plan d'action de mise en oeouvre des mesures de sécurité

Conclusion :

Après avoir suivre les cinq modules de la méthode EBIOS on a réussi à établir les documents suivants :

- ✓ La politique de sécurité. (Annexe A)
- ✓ Déclaration d'applicabilité : Les bonnes pratiques de la norme ISO/IEC 27002 appliqué au sein de l'entreprise et leur description être conforme à la norme ISO/IEC 27001.

La description des bonnes pratiques qui manquent sont détaillées dans la partie suivante de ce chapitre.

Partie 2 : présentation de la solution UNICOM.

Introduction :

Après avoir analysé les systèmes d'information et les mesures de sécurités existants chez UNIDEES, on a trouvé qu'il ne répand pas à tous les bonnes pratiques de la norme ISO/ IEC 27002, donc on a établi la politique de sécurité et crée une application pour assurer la continuité de l'amélioration en premier lieu, puis la communication entre le responsable de sécurité et le reste des employés.

1. Conception de l'application :

1. Le langage UML :

Le langage de modélisation unifié, de l'anglais Unified Modeling Language (UML), est un langage de modélisation graphique à base de pictogrammes conçu pour fournir une méthode normalisée pour visualiser la conception d'un système. Il est couramment utilisé en développement logiciel et en conception orientée objet.

L'UML est le résultat de la fusion de précédents langages de modélisation objet : Booch, OMT, OOSE. Principalement issu des travaux de Grady Booch, James Rumbaugh et Ivar Jacobson, UML est à présent un standard adopté par l'Object Management Group (OMG). [20]

2. Diagramme de cas d'utilisation :

Les diagrammes de cas d'utilisation sont des diagrammes UML utilisés pour donner une vision globale du comportement fonctionnel d'un système logiciel. Ils sont utiles pour des présentations auprès de la direction ou des acteurs d'un projet, mais pour le développement, les cas d'utilisation sont plus appropriés. [20]

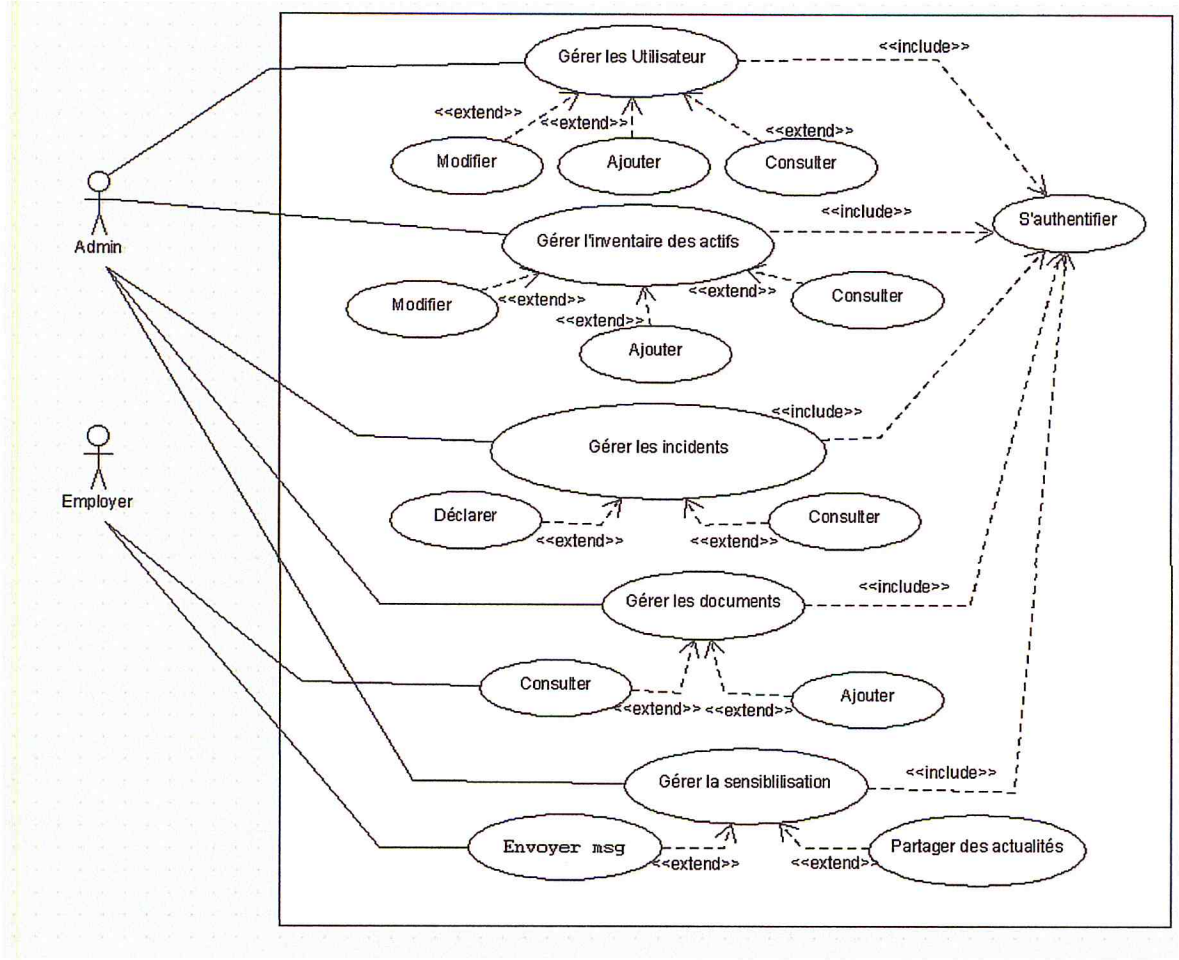


Figure 15 Diagramme de cas d'utilisation générale.

Description des opérations principales du diagramme de cas d'utilisation :

Notre application a pour but d'aider les responsables de sécurité à la création de la liste des biens (actifs) et documenté toutes modifications et règles d'utilisation de ces derniers et pour plus d'informations voir la description de capture de l'application.

3. Diagramme de classe :

Le diagramme de classe est une représentation statique des éléments qui composent un système et de leurs relations. Chaque application qui va mettre en œuvre le système sera une instance des différentes classes qui le compose. [20]

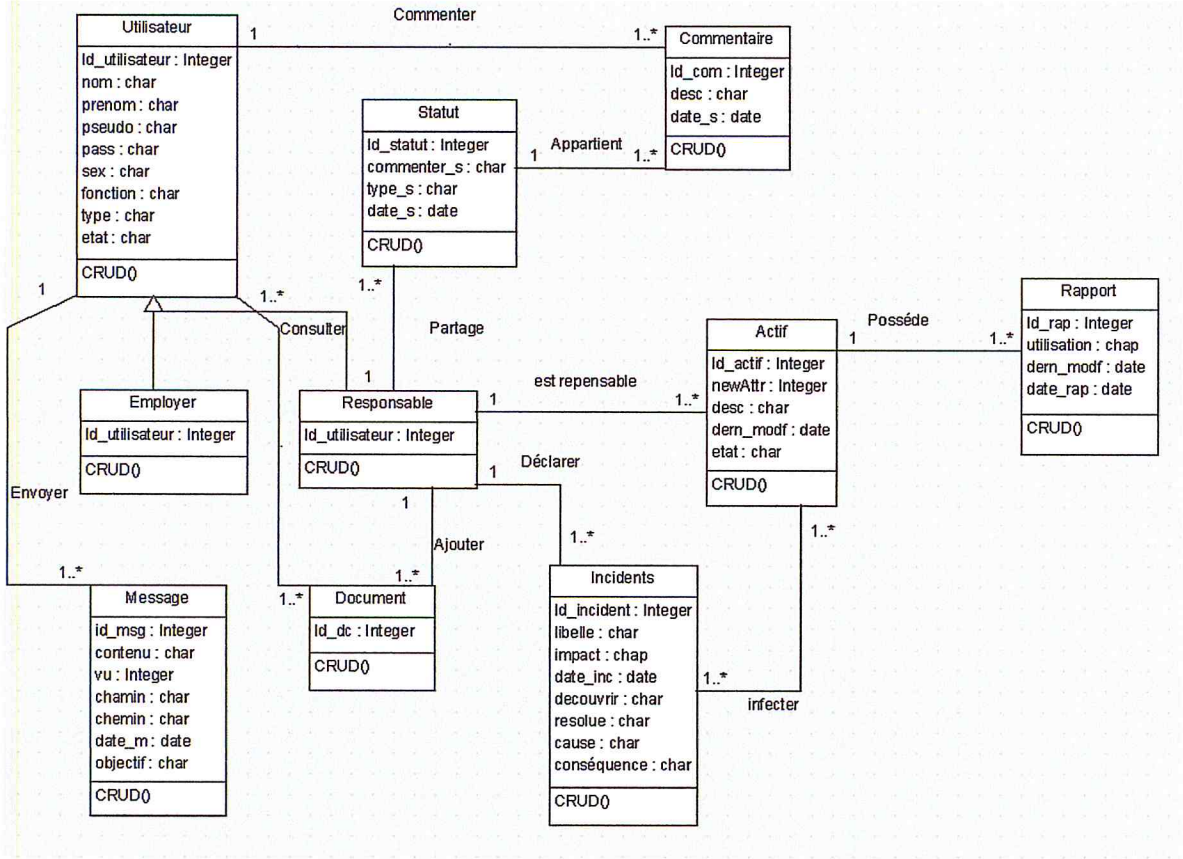


Figure 16 Diagramme de classe

4. L'environnement de développement :

1. WAMPSever :

WAMPSever est une plate-forme de développement Web sous Windows pour des applications Web dynamiques à l'aide du serveur Apache2, du langage de scripts PHP et d'une base de données MySQL. Il possède également PHPMyAdmin pour gérer plus facilement vos bases de données. [21]

2. Langage HTML :

L'HTML est un langage informatique utilisé sur l'internet. Ce langage est utilisé pour créer des pages web. L'acronyme signifie HyperText Markup Language, ce qui signifie en français "langage de balisage d'hypertexte". Cette signification porte bien son nom puisqu'effectivement ce langage permet de réaliser de l'hypertexte à base d'une structure de balisage. [22]

3. Langage PHP :

PHP est un langage de programmation qui s'intègre dans vos pages HTML. Il permet entre autres de rendre automatiques des tâches répétitives, notamment grâce à la communication avec une base de données (utilisation la plus courante de PHP). [23]

4. Le CSS :

Le terme CSS est l'acronyme anglais de Cascading Style Sheets qui peut se traduire par "feuilles de style en cascade". Le CSS est un langage informatique utilisé sur l'internet pour mettre en forme les fichiers HTML ou XML. Ainsi, les feuilles de style, aussi appelé les fichiers CSS, comprennent du code qui permet de gérer le design d'une page en HTML. [24]

5. Le langage SQL :

SQL (sigle de Structured Query Language, en français langage de requête structurée) est un langage informatique normalisé servant à exploiter des bases de données relationnelles.

Les instructions de manipulation du contenu de la base de données commencent par les mots clés SELECT, UPDATE, INSERT ou DELETE qui correspondent respectivement aux opérations de recherche de contenu, modification, ajout et suppression. Divers mots clés tels que FROM, JOIN et GROUP permettent d'indiquer les opérations d'algèbre relationnelle à effectuer en vue d'obtenir le contenu à manipuler. [24]

Présentation des interfaces de l'application :

1. L'interface d'ajout un actif :

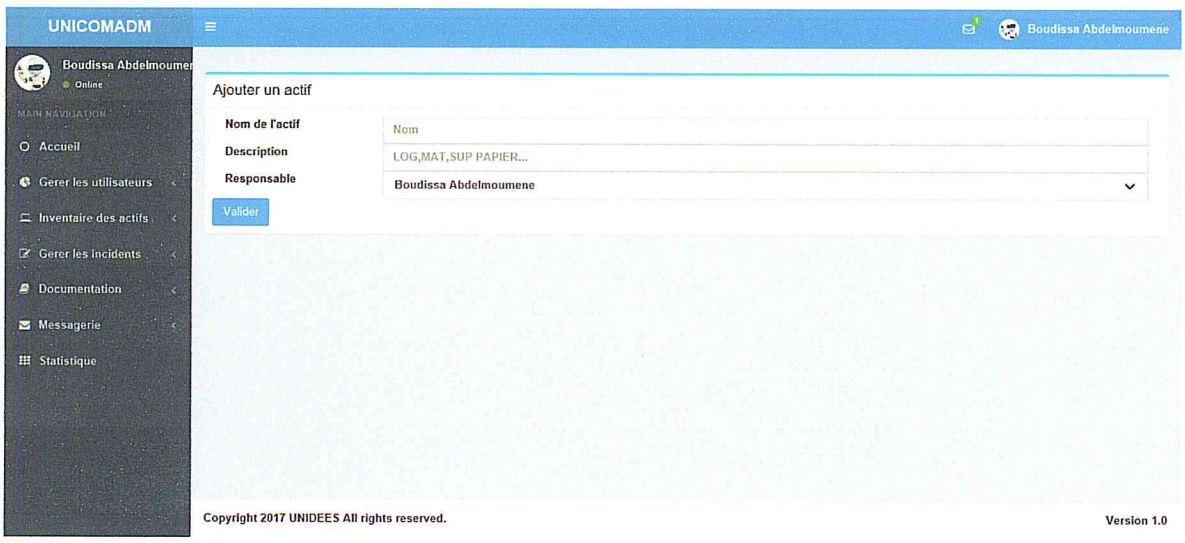


Figure 17 Interface [ajouter un actif]

L'interface de création d'un rapport d'un actif :

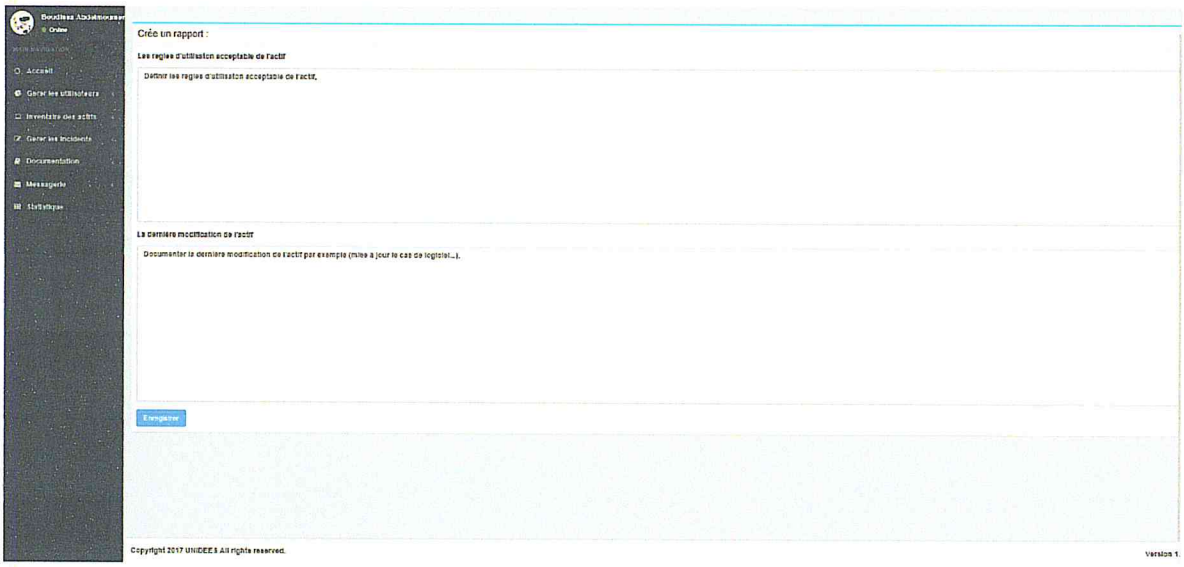


Figure 18 Interface [crée un rapport d'un actif]

Inventaire des actifs (biens) :

ISO/CEI 27002 à spécifier tout un chapitre pour la réalisation de la gestion des actifs (chapitre 8) :

- ✓ Identifier les actifs de l'entreprise et définir les responsabilités de protection appropriées :
  - Les actifs liés aux installations de traitement de l'information et de l'information doivent être identifiés et un inventaire de ces actifs doit être établie et maintenue.
  - Définir un propriétaire pour chaque actif.
  - Règles relative à l'utilisation acceptable des actifs.
- ✓ Assurer que l'information reçoit un niveau de protection appropriée conformément à son importance pour l'organisation.

2. L'interface de l'accueil Responsable(Admin) et messagerie

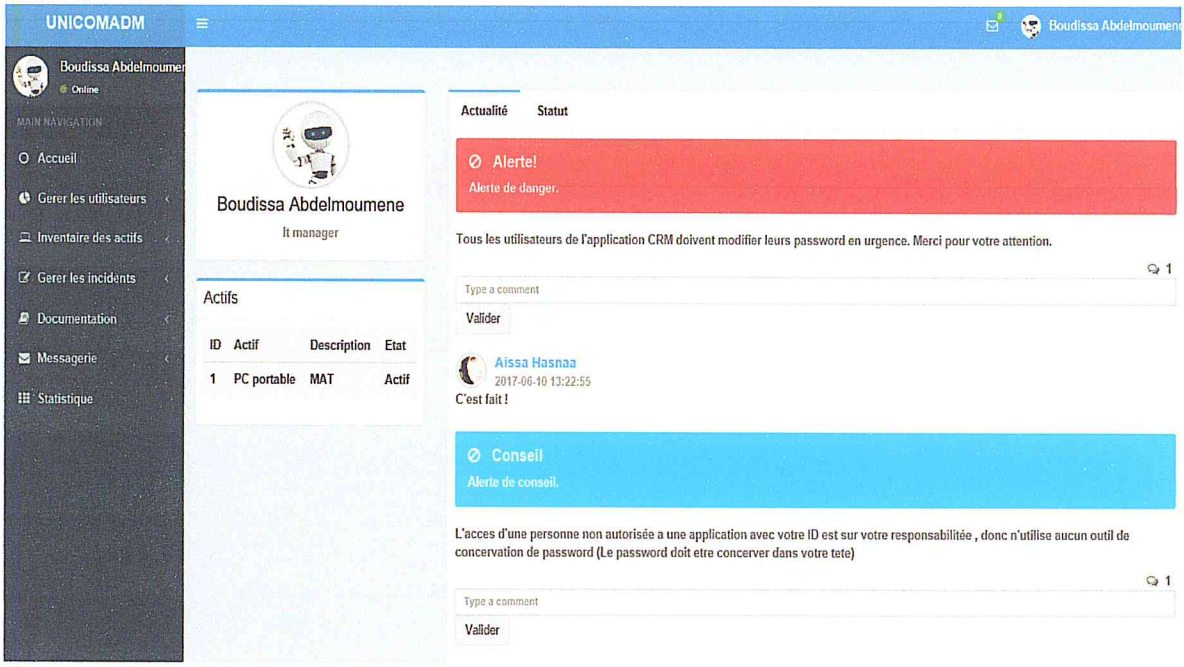


Figure 19 Interface [accueil Responsable(Admin)]

L'interface de messagerie :

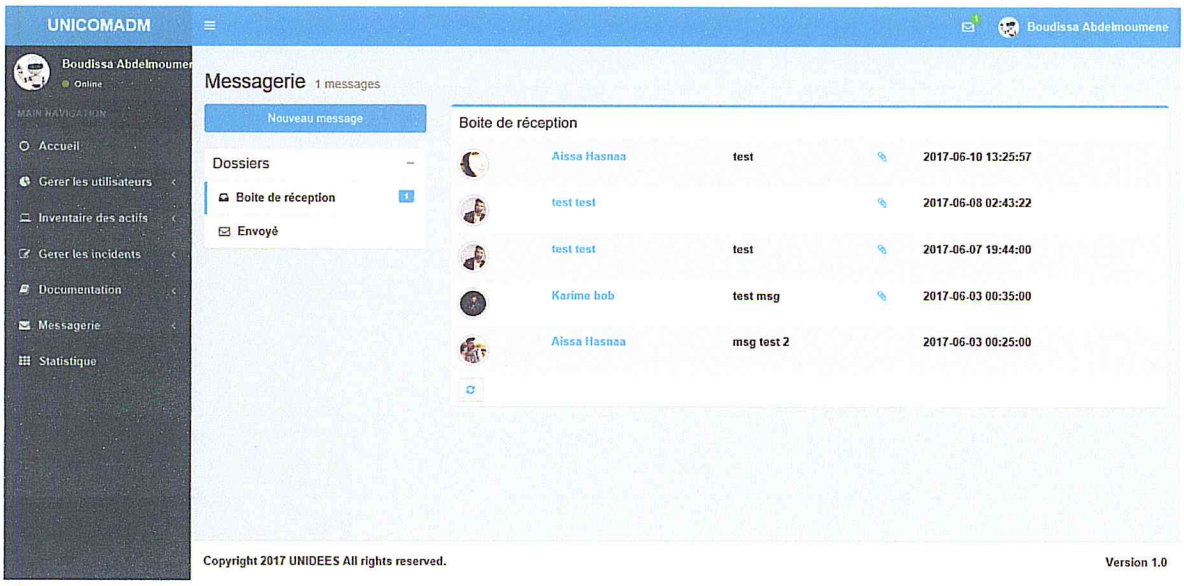


Figure 20 Interface [messagerie]

Communication :

La communication est une partie de chapitre 7 (support) de la norme ISO/IEC 27001 et notre application garantie un moyen de communication entre les responsables de sécurités et les employés :

- ✓ Sur ce qu'il faut communiquer :
  - Un impact sérieux sur les objectifs stratégiques à long terme.
  - Les détails du changement à toutes les personnes concernées.
  - Les risques.
  - La sensibilisation (7.2.2 ISO/IEC 27002).

3. L'interface d'ajout un incident :

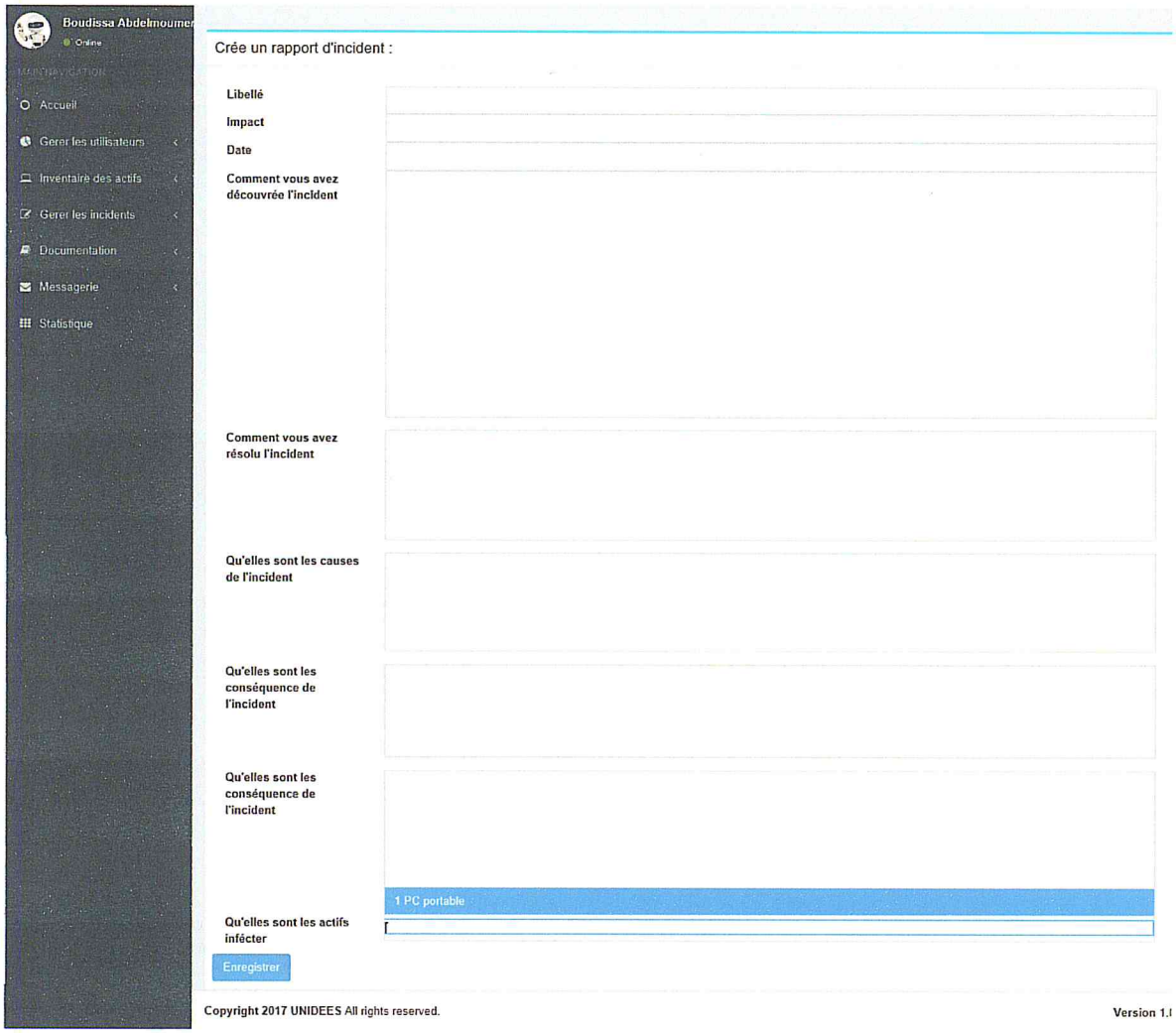


Figure 21 Interface [déclarer un incident]

Gestion des incidents :

- ✓ Déclarer et documenté les incidents de sécurité de l'information en spécifiant comment il a été détecté et comment il a été résolu.

Notre application a pour but d'aider les responsables de sécurité à la création des rapports sur les incidents et les consulter après.

4. L'interface de consulter document :

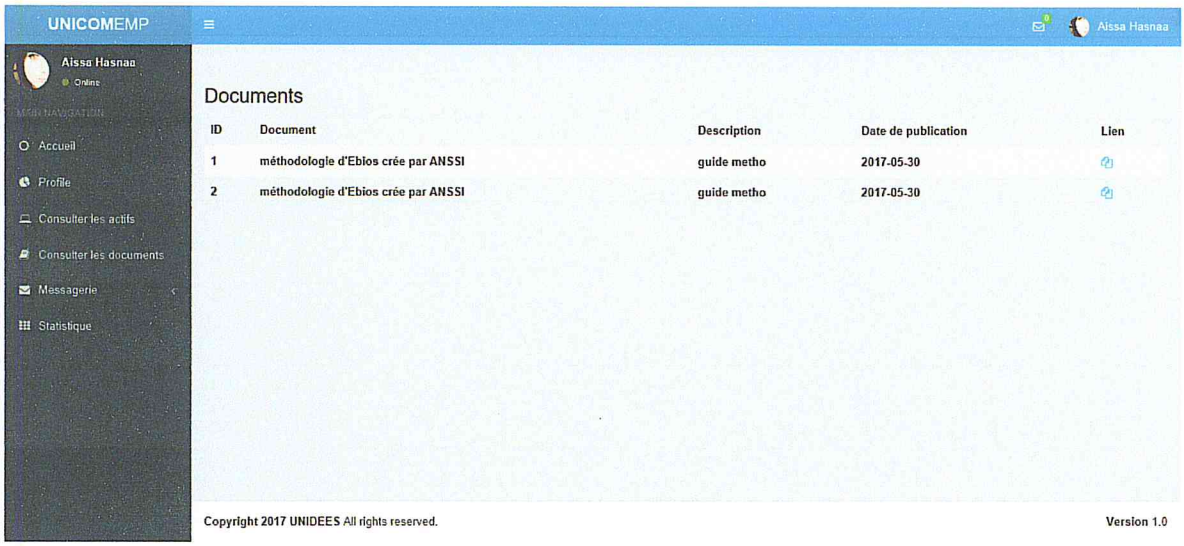


Figure 22 Interface [consulter document]

Documents :

- ✓ Publier les documents relatifs à la sécurité de l'information.
- ✓ Assurer la disponibilité de ces documents (consultation).

Note : Notre application garantie l'organisation des documents en matière de sécurité de l'information (création, publication, consultation, accès sécurisé).

Conclusion :

Cette partie a été consacrée à l'implémentation de notre solution pour la gestion de la continuité de la sécurité des systèmes d'information. En premier lieu nous avons établir une politique de sécurité. Ensuite nous avons entamé l'application qui géré le reste de mesures de sécurité qui manque dans l'entreprise pour être conforme à la série des normes ISO/IEC 2700x.

Nous avons abouti au terme de ce travail à un résultat conforme aux attentes des utilisateurs (responsables de sécurité et le reste des employés chez UNIDEES), et à un système qui reste extensible et évolutif, ce qui permettra de l'adapter à d'autres entreprises.

Conclusion générale :

Le présent travail à porter sur la réalisation d'un système de management de sécurité de l'information conforme aux exigences de la norme ISO/IEC 27001, en suivant la méthode EBIOS pour la gestion des risques et la sélection de mesures de sécurité de la norme ISO/IEC 27002.

Nous avons donc découvrir le monde des normes international ou on a travaillé avec la série ISO/IEC 2700x, mais on juste choisie ISO/IEC (27001/27002/ 27003/ 27005) il sera bien de continue l'étude de la sécurité prochainement selon cette série ou on va la terminé par l'étude du reste de la série ISO/IEC (27004/27006/27007).

A la fin, nous sommes satisfais avec le thème choisi, car la réalisation de ce projet nous a été bénéfique à tous les niveaux et nous a permis de découvrir le domaine des normes internationaux en matière de sécurité de l'information, domaine vaste et en pleine expansion.

Références bibliographique :

- [1] Site web officiel de l'entreprise UNIDEES http://www.unidees.dz/ Consulter le 20/04/2017.
- [2] https://www.pcssansvius.com/pages pare-feu matériel. Consulter le 30/04/2017.
- [3] Site web officiel de Kaspersky endpoint 10 http://www.support.kaspersky.com/ Consulter le 20/04/2017.
- [4] Site web officiel de OWASP 10 http://www.owasp.org/waf Consulter le 19/04/2017.
- [5] Site web officiel de OWASP 10 http://www.owasp.org/ Consulter le 21/04/2017.
- [6] Site web officiel de WALLIX 10 http://www.wallix.com/ Consulter le 18/04/2017.
- [7] https://www.ysosecure.com/ Consulter le 15/04/2017.
- [8] http://www.isaca.org Consulter le 10/04/2017.
- [9] [ISO 27000] Information technology — Security techniques — Information security management systems — Overview and vocabulary ISO (2016).
- [10] [ISO 27001] Information technology – Security Techniques – Information security management systems – Requirements, International Organization for Standardization – ISO (2013).
- [11] [ISO 27002] Information technology – Code of practice for information security management, International Organization for Standardization – ISO (2013).
- [12] [ISO 27003] Information technology — Security techniques — Information security management system implementation guidance ISO (2010).
- [13] [ISO 27004] Information technology — Security techniques — Information security management — Measurement ISO (2009).
- [14] [ISO 27005] Information technology — Security techniques — Information security risk management ISO (2011).
- [15] [ISO 27006] Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems ISO (2015).
- [16] [ISO 27007] Information technology — Security techniques — Guidelines for information security management systems auditing ISO (2011).
- [17] Site web officiel de ISO http://www.iso.com/ page consulté le 10/06/2017.

- [18] Expression des Besoins et Identification des Objectifs de Sécurité EBIOS MÉTHODE DE GESTION DES RISQUES (http://www.ssi.gouv.fr).
- [19]
- [20] Natalie GAERTNER Pierre-Alain Muller. Modalisation objet avec UML. Eyrolles Edition, Avril 2010.
- [21] Site web officiel de WAMPSever http://www.wampserver.com/ page consulté le 19/05/2017.
- [22] Maitrise des CSS, Andy BuddBudd avec Cameron Mall et Simon Collison, 2eme Edition, 2009.
- [23] Pratique de MYSQL et PHP, Philippe Rigaux. 4em Edition Dunod, Paris, 2009.

POLITIQUE DE SECURITE UNIDEES

Version 1.0

19 MAI 2017

UNIDEES Algérie

Service de sécurité informatique à Baba Hassen, Algérie

HISTORIQUE DES VERSIONS		
DATE	**VERSION**	**ÉVOLUTION DU DOCUMENT**
19/05/2017	1.0	Publication de la première version de la Politique de sécurité des systèmes d'information de l'Etat.

Politique de sécurité

1. Introduction :

La politique de sécurité des systèmes d'information d'UNIDEES contribue à :

- assurer la continuité des activités régaliennes ;
- prévenir la fuite d'informations sensibles ;
- renforcer la confiance des clients et des partenaires.

Le présent document définit les mesures de sécurité applicables aux systèmes d'information d'UNIDEES Algérie.

La PS s'adresse à l'ensemble des agents de l'État, et tout particulièrement aux responsables de sécurité de l'information.

Première Partie : instruction

2. Objectif de la PS :

La présente instruction fixe les conditions de mise en œuvre de la politique de sécurité des systèmes d'information d'UNIDEES.

3. Champ d'application :

La PS s'applique à tous les systèmes d'information (SI) tous trois directions (Administrative, Technique, Commercial).

La PS concerne l'ensemble des personnes physiques ou morales intervenant dans ces SI, qu'il s'agisse des administrations d'UNIDEES et de leurs agents ou bien de tiers (prestataires ou sous-traitants) et de leurs employés.

La plupart des règles de sécurité de la PS constituent des règles de base qui devraient pouvoir être appliquées plus largement, au-delà des administrations d'UNIDEES.

4. Dispositions transitoires :

La mise en application de la PS s'effectue selon les règles suivantes :

- les SI des administrations de l'UNIDEES devront être en conformité totale dans les trois ans suivant la publication de la PS ;
- les entités devront, au 1er janvier 2018, avoir mis en conformité leur politique de sécurité des systèmes d'information (PSSI) et défini un plan d'action. Celui-ci tiendra compte des impacts sur les activités ainsi que des moyens financiers et humains à mettre en œuvre. Il sera établi un calendrier de mise en conformité indiquant les mesures à prendre dans l'immédiat puis à court et à long terme.

5. Formation des agents

Les administrateurs forment leurs agents chargés d'appliquer la PS. Ces derniers doivent être sensibilisés à la sécurité des SI (SSI) et au respect des règles de sécurité. Les agents exploitant les SI ou assurant des missions en lien avec la SSI font l'objet de formations adaptées, dispensées par les responsables eux-mêmes.

6. Pilotage et évolutions de la PS

La PS est amené à évoluer dans le temps. Elle pourra notamment être revue afin de prendre en compte :

- les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- les résultats d'analyses de risques ainsi que les actions découlant de contrôles ou d'inspections ;
- les évolutions des contextes organisationnel, juridique, réglementaire et technologique.

7. Traitement des incidents et gestion de crise

La rapidité des attaques informatiques rend nécessaire une veille renforcée et une réaction coordonnée des différents acteurs. Afin de rétablir le fonctionnement rapide des activités vitales de l'UNIDEES, une stratégie de traitement des incidents et de gestion de crise est mise en place.

L'ensemble des acteurs (utilisateurs, responsables d'applications, des réseaux et des serveurs ....) doit remonter tout événement affectant ou pouvant affecter la disponibilité, l'intégrité, la confidentialité ou la traçabilité des systèmes d'information d'une entité. Ces incidents de sécurité doivent être signalés rapidement à la technique.

Une situation d'urgence SSI résulte de toute alerte ou incident sur un ou plusieurs SI générant un dysfonctionnement majeur des activités de l'entreprise. Une situation de cette nature impose une forte réactivité et une coordination planifiée des différents acteurs concernés.

Deuxième Partie : objectifs et règles

1. Organisation de la sécurité des systèmes d'information

Objectif 1 : organisation de la SSI. Mettre en place une organisation adéquate, garantissant la prise en compte préventive et réactive de la sécurité.

2. Ressources humaines

Objectif 2 : ressources humaines. Faire des personnes les maillons forts des SI de l'entreprise.

1. Personnel permanent

- RH-MOTIV : choix et sensibilisation des personnes tenant les postes clés de la SSI. Une attention particulière doit être portée au recrutement des personnes-clés de la SSI : RSSI, correspondants SSI locaux et administrateurs de sécurité. Les RSSI et leurs correspondants SSI locaux doivent être spécifiquement formés à la SSI. Les administrateurs des SI doivent être régulièrement sensibilisés aux devoirs liés à leur fonction, et doivent veiller à respecter ces exigences dans le cadre de leurs activités quotidiennes.
- RH-CONF : personnels de confiance. Toutes les personnes manipulant des informations sensibles doivent le faire avec une attention et une probité particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées.
- RH-UTIL : sensibilisation des utilisateurs des systèmes d'information. Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant, et motivé à leur respect. Il doit être formé à l'utilisation des outils de travail conformément aux règles SSI.

2. Mouvement de personnel

RH-MOUV : gestion des arrivées, des mutations et des départs. Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs dans les SI doit être formalisée, et appliquée strictement. Cette procédure doit couvrir au minimum :

- la gestion/révocation des comptes et des droits d'accès aux SI, y compris pour les partenaires et les prestataires externes ;
- la gestion du contrôle d'accès aux locaux ;
- la gestion des équipements mobiles ;
- la gestion du contrôle des habilitations.

3. Personnel non permanent

RH-NPERM : gestion du personnel non permanent (stagiaires, intérimaires, prestataires...). Les règles de la PSSIE s'appliquent à tout personnel non permanent utilisateur d'un SI d'une administration de l'État. Les dispositions contractuelles préexistantes régissant l'emploi de ce personnel sont amendées si nécessaire. Pour tout personnel non permanent, un tutorat par un agent permanent est mis en place, afin de l'informer de ces règles et d'en contrôler l'application.

4. Gestion des biens

Objectif 3 : cartographie des SI. Tenir à jour une cartographie détaillée et complète des SI.

GDB-INVENT : inventaire des ressources informatiques. Chaque entité établit et maintient à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire est tenu à disposition du RSSI. Il comprend la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes. Il est constitué d'une base de données de configuration, maintenue à jour et tenue à disposition du RSSI.

GDB-CARTO : cartographie. La cartographie précise les centres informatiques, les architectures des réseaux (sur lesquelles sont identifiés les points névralgiques et la sensibilité des informations manipulées) et qualifie le niveau de sécurité attendu. Cette cartographie est maintenue à jour et tenue à disposition du RSSI.

Objectif 4 : qualification et protection de l'information. Qualifier l'information de façon à adapter les mesures de protection.

GDB-QUALIF-SENSI : qualification des informations. La sensibilité de toute information doit être évaluée. Le marquage systématique des documents, en fonction du niveau de sensibilité, est fortement recommandé.

GDB-PROT-IS : protection des informations. L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie, depuis la création du brouillon jusqu'à son éventuelle destruction.

5. Intégration de la SSI dans le cycle de vie des systèmes d'information :

1. Gestion des risques et homologation de sécurité

Objectif 5 : risques. Apprécier, traiter, et communiquer sur les risques relatifs à la sécurité des systèmes d'information.

INT-HOMOLOG-SSI : Homologation de sécurité des systèmes d'information. Tout système d'information doit faire l'objet d'une décision d'homologation de sa sécurité avant sa mise en exploitation dans les conditions d'emploi définies. L'homologation est l'acte selon lequel l'autorité atteste formellement auprès des utilisateurs que le système d'information est protégé conformément aux objectifs de sécurité fixés. La décision d'homologation est prise par l'autorité d'homologation (désignée par l'autorité qualifiée), le cas échéant après avis de la commission d'homologation. Cette décision s'appuie sur une analyse de risques adaptée aux enjeux du système considéré, et précise les conditions d'emploi.

2. Maintien en condition de sécurité des systèmes d'information

Objectif 6 : maintien en condition de sécurité. Gérer dynamiquement les mesures de protection, tout au long de la vie du SI.

INT-SSI : intégration de la sécurité dans les projets. La sécurité des systèmes d'information doit être prise en compte dans toutes les phases des projets informatiques, sous le contrôle de l'autorité d'homologation, de la conception et de la spécification du système jusqu'à son retrait du service.

1. 6. Sécurité physique

2. Sécurité physique des locaux abritant les SI

L'objectif est d'empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux dans lesquels résident les informations de l'unité. Les locaux contenant des informations

sensibles et des moyens de traitement de l'information (salles serveurs, secrétariat de direction ou d'enseignement…) doivent donc être protégés physiquement des accès incontrôlés ou malveillants (contrôle d'accès par carte ou code).

Pour se protéger des menaces d'ordre environnemental, il convient également de mettre en œuvre des dispositifs de détection et d'alerte de température élevée, d'incendie ou d'inondations ou d'autres formes de sinistres provoqués soit accidentellement soit par malveillance.

3. Sécurité du matériel et du câblage :

On protégera les matériels sensibles (routeurs, serveurs…) des pertes d'alimentation électrique par un système de secours bien dimensionné, ainsi que d'éventuelles surchauffes par des moyens de climatisation adéquats et bien dimensionnés.

Afin de garantir une disponibilité permanente et un bon fonctionnement en cas de panne, le matériel sensible qui nécessite un fonctionnement continu doit être placé sous contrat de maintenance.

Les accès aux câbles réseaux transportant des données doivent être protégés contre toute possibilité d'interception de l'information, ou de dommage. Les câbles ou concentrateurs réseaux doivent être hors de portée immédiate et donc protégés dans des gaines ou des armoires de répartition.

4. Mise au rebut ou recyclage

Les matériels, les informations ou les logiciels ne devraient pas pouvoir être sortis des unités sans autorisation préalable au vu d'une procédure formelle. En cas de mise au rebut ou de revente de PC, il convient de vérifier que les données ont été effacées des disques de manière efficace. Un simple formatage n'étant bien entendu pas suffisant pour effacer les données de manière pérenne, des méthodes sont préconisées.

Les supports qui ne servent plus doivent être mis au rebut de façon sûre. Il n'est pas conseillé pour des raisons environnementales de même que pour des raisons de sécurité du SI de se débarrasser des PC et des supports amovibles dans des bennes non spécialisées, ni sans avoir au préalable correctement effacé les supports (magnétiques, etc.).

5. Procédures de sécurité informatique liées à l'exploitation

Protection contre les codes malveillants : virus et autres « malwares »

La plupart des attaques via le réseau tentent d'utiliser les failles du système d'exploitation ou des logiciels d'un PC. Les attaques recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parvenir à s'y introduire.
C'est pourquoi il est fondamental que les ASR mettent à jour les logiciels des serveurs et des postes clients afin de corriger ces failles.

L'ASR doit veiller au maintien du niveau de sécurité au cours du temps par l'application récurrente des correctifs logiciels (*patchs*) sur les serveurs en exploitation dans l'unité.

Il est également dans ses fonctions, de veiller à ce que chaque poste du réseau local soit équipé d'un antivirus régulièrement mis à jour. L'ASR doit donc mettre en place des mesures de détection, de prévention et de recouvrement pour se protéger des codes malveillants.

Sauvegarde des informations

La sauvegarde des informations est un processus essentiel permettant de garantir la disponibilité des données et la continuité de l'activité du laboratoire en cas d'incident. Une sauvegarde régulière des

données des utilisateurs ainsi qu'un processus de restauration, testés au préalable, doivent être mis en place. Les droits d'accès à ces sauvegardes doivent faire l'objet d'une attention particulière.

Des copies de ces sauvegardes doivent être réalisées sur des supports externes (robot de bandes, disques externes…) et placées dans des locaux (ou coffres) sécurisés et distants. Ces copies de sauvegardes doivent aussi être testées régulièrement conformément à la politique de sauvegarde convenue.

Journaux systèmes – les logs

Les journaux systèmes produits par nos serveurs informatiques permettent la surveillance du contrôle d'accès à nos systèmes et réseaux. Ils permettent de faciliter les investigations ultérieures et sont en outre également exigés dans le cadre de la collecte de preuve par les autorités juridiques compétentes.

Les journaux systèmes qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité doivent être produits et conservés pendant la période légale pour surveiller l'exploitation du système.

Synchronisation des horloges

En cas d'analyse des journaux informatiques, pour retracer la chronologie d'un événement ou d'une anomalie, il est essentiel que les horloges des différents systèmes de traitement de l'information (serveurs, routeurs, PC utilisateurs…) de l'entreprise de recherche soient synchronisées à l'aide d'une source de temps précise et préalablement définie.

Sécurité du réseau – Echange des informations – Contrôle d'accès réseau

Les réseaux d'UNIDEES doivent être gérés et contrôlés de manière adéquate pour garantir la protection contre des menaces aussi bien externes qu'internes. On veillera surtout à contrôler l'accès physique au réseau, segmenter le réseau local en différents réseaux virtuels et à rendre illisibles notamment les informations en transit, par des moyens de chiffrement des protocoles :

- contrôle d'accès réseau : il est nécessaire d'empêcher les accès non autorisés aux services qui sont disponibles sur le réseau (partages de dossiers, imprimantes, accès intranet, web, etc.). L'ASR doit s'assurer de ne donner accès qu'aux services pour lesquels les utilisateurs ont spécifiquement reçu une autorisation. Des méthodes d'authentification appropriées doivent donc être utilisées pour contrôler l'accès des utilisateurs distants. La mise en place d'annuaires centralisés tels que *Active Directory* ou LDAP représente un élément fondamental pour permettre cette authentification ;
- cloisonnement des réseaux : La segmentation du réseau de l'unité en réseaux logiques virtuels (VLAN) est donc une bonne mesure à prendre pour séparer des flux réseau de différentes entités administratives (le réseau des chercheurs, le réseau des étudiants, le réseau de secrétariats, le réseau des serveurs…). Cette différenciation des flux permet, par la suite, de leur appliquer des mesures de sécurité différentes. Dans le processus de segmentation du réseau, il est fortement recommandé de regrouper et d'isoler les services devant être visibles de l'extérieur dans une zone réseau « semi ouverte » ;
- contrôle du routage réseau : le réseau hébergeant le SI doit être protégé des tentatives d'accès illicites provenant de l'extérieur comme de l'intérieur de nos unités. Des mesures de routage des réseaux doivent être mises en œuvre afin d'éviter que des connexions réseau non souhaitées ne portent atteinte à la politique de contrôle d'accès des applications métier de nos unités. Les flux d'entrée, et de sortie, du réseau doivent également être protégés par un ensemble de filtres

(ACL dans le jargon) qui permettent d'interdire des accès réseau vers des ressources ou des services non contrôlés.

Protection des transferts de données : chiffrement

L'objectif des mesures cryptographiques est de protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des algorithmes utilisant des clés de chiffrement.

Il est important pour les ASR de connaître le fonctionnement de l'Infrastructure de Gestion de Clé (IGC) de leur structure lorsqu'elle existe et l'utilisation que l'on peut faire des certificats délivrés (signature et chiffrement des messages électroniques, certification de machines serveurs...).

Exigences relatives au contrôle d'accès aux systèmes d'exploitation

Une procédure formelle de création (et de suppression) des comptes informatiques des utilisateurs destinée à accorder ou à supprimer l'accès à tous les systèmes et services d'information doit être définie. Après création des comptes, il est nécessaire de gérer correctement l'attribution et l'utilisation des privilèges.

L'accès aux ressources informatiques ne doit donc être possible qu'après identification et authentification des utilisateurs et doit être adapté aux droits et aux profils des utilisateurs (chercheurs, administration, enseignement, etc.).

L'ASR attribue un identifiant et un mot de passe unique à chaque utilisateur et met en place le système d'authentification adéquat, pour vérifier l'identité déclarée par l'utilisateur lors des entrées en session.

Les utilisateurs doivent pouvoir changer leur mot de passe à partir d'un processus formel contrôlé de manière à empêcher l'utilisation de mots de passes trop faibles (utiliser des mots ne figurant pas dans un dictionnaire et difficiles à retrouver à l'aide de programmes).

Il est important de faire adhérer les utilisateurs à ces mesures qui peuvent paraître contraignantes, mais qui figurent parmi les mesures de base permettant d'assurer la sécurité de l'accès au système d'information des unités.

Dans certains contextes (salles d'enseignements ou applications sensibles...) les sessions inactives devraient être déconnectées après une période d'inactivité définie.

Gestion de parc et des moyens nomades – Cybersurveillance

L'administration des postes de travail de nos unités est normalement placée sous la responsabilité de l'ASR. Selon la réglementation en vigueur actuellement, il a donc toute latitude pour mettre en place des outils de gestion et de surveillance du parc informatique. Ainsi, une vérification du niveau de sécurité des postes nomades (présence d'un antivirus à jour par exemple) doit être mise en place avant l'accès au réseau local. Les postes de travail et moyens nomades doivent par ailleurs être protégés par des mots de passe robustes.

En cas de télémaintenance sur un PC avec des outils de prise en main à distance tel que VNC, les ASR doivent avertir le propriétaire du poste et respecter la législation.

6. Sauvegarde et archivage

Une des fonctions de l'ASR est de proposer des dispositifs qui permettent d'assurer une préservation de ces données en cas de perte accidentelle ou autre. La duplication de ces données par stockage redondant sur des supports différents de ceux de l'équipement utilisé (poste de travail fixe, mobile,

serveur, ...) est un des principes de base. Elle nécessite la mise en place de techniques et de procédures de stockage et de restauration spécifiques au type de donnée concernée.

Il convient donc de distinguer clairement les deux finalités :

- la sauvegarde, quel que soit sa forme et son usage, est destinée à mémoriser des données évolutives de manière à en conserver la persistance et pouvoir les restituer en cas d'accident. On peut couramment considérer que les données stockées sont régulièrement modifiées (écrites, effacées) ;
- l'archivage, en revanche, consiste à rendre accessible en lecture des données immuables (archives de documents administratifs, données de mesures expérimentales, résultats de simulations coûteuses à produire, etc.), bien que leur classification puisse évoluer dans le temps (métadonnées associées).

7. Respecter la législation

Il n'existe pas des exigences législatives concernant la sécurité des systèmes d'informations.

8. Formation, sensibilisation

La formation, la sensibilisation et l'information des différents acteurs de l'expert SSI à l'utilisateur en passant par le responsable de l'entité sont cruciales pour la sécurité. Sous la responsabilité de la chaîne fonctionnelle SSI, des actions en ce sens sont régulièrement menées au niveau local, régional et national.

Elles font l'objet d'une planification arrêtée au niveau du comité de pilotage de la SSI et donnent lieu à un suivi dans le cadre du tableau de bord de la SSI.

9. Règles de sécurité complémentaires s'appliquant aux salles informatiques et aux locaux techniques

PHY-CI-ENERGIE : local énergie. L'alimentation secteur des équipements devra être conforme aux règles de l'art, de façon à se prémunir des atteintes à la sécurité des personnes et équipements liées à un défaut électrique.

PHY-CI-CLIM : climatisation. Un dispositif de climatisation dimensionné en fonction des besoins énergétiques du système informatique doit être installé. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

PHY-CI-INC : lutte contre l'incendie. L'installation de matériel de protection contre le feu est obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier, ou autre source potentielle de départ de feu ne doit être entreposé dans ces locaux.

PHY_CI-EAU : lutte contre les voies d'eau. Une étude sur les risques dus aux voies d'eau doit être réalisée. Cette étude doit notamment prendre en compte le risque de fuite sur un collecteur d'eau douce.

10. SI de sûreté

Objectif 6 : sécurité du SI de sûreté. Traiter de manière globale la sécurité des systèmes d'information et de communication qui assurent la sûreté d'un site.

PHY-SI-SUR : sécurisation du SI de sûreté. Pour les sites physiques considérés comme importants, des mesures de protection doivent être définies et appliquées en se basant sur les conclusions d'une analyse de risques. L'analyse de risques conduit à la désignation des briques essentielles dont il faut assurer la protection contre des actes malveillants. Un système de gestion de la sécurité du SI de sûreté (s'inspirant de la norme ISO 27001) assure le maintien en condition de sécurité. L'emploi de produits labellisés, quand ils existent, est fortement recommandé.

11. Sécurité des réseaux

1. Sécurité des réseaux locaux

Objectif 7 : usage sécurisé des réseaux locaux. Maîtriser les interconnexions de réseaux locaux. Configurer de manière adéquate les équipements de réseau actifs.

RES-CLOIS : cloisonner le SI en sous-réseaux de niveaux de sécurité homogènes. Par analogie avec le cloisonnement physique d'un bâtiment, le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.

2. Sécurité des réseaux sans fil

Objectif 8 : usage sécurisé des réseaux sans fil. Maîtriser le déploiement, la configuration et l'usage des réseaux sans fil.

RES-SSFIL : mise en place de réseaux sans fil. Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires, doivent être prises dans le cadre de la défense en profondeur.

3. Sécurisation des mécanismes de commutation et de routage

Objectif 9 : sécurité des mécanismes de commutation et de routage. Configurer les mécanismes de commutation et de routage pour se protéger des attaques.

4. Cartographie réseau

Objectif 10 : cartographie réseau. Tenir à jour une cartographie détaillée et complète des réseaux et des interconnexions.

5. Sécurité du poste de travail

1. Sécurisation des postes de travail

Objectif 11 : sécurisation des postes de travail. Durcir les configurations des postes de travail en protégeant les utilisateurs.

2. Mise à disposition du poste

PDT-GEST : fourniture et gestion des postes du travail. Les postes de travail utilisés dans le cadre professionnel sont fournis et gérés par l'équipe locale chargée des SI.

3. Sécurité physique des postes de travail

PDT-VEROUIL-FIXE : verrouillage de l'unité centrale des postes fixes. Lorsque l'unité centrale d'un poste fixe est peu volumineuse, donc susceptible d'être facilement emportée, elle doit être protégée contre le vol par un système d'attache (par exemple un câble antivol).

PDT-VEROUIL-PORT : verrouillage des postes portables. Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation.

4. Gestion des privilèges sur les postes de travail

PDT-PRIVIL : privilèges des utilisateurs sur les postes de travail. La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe du « moindre privilège » : chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.

PDT-PRIV : utilisation des privilèges d'accès « administrateur ». Les privilèges d'accès « administrateur » doivent être utilisés uniquement pour les actions d'administration le nécessitant.

5. Protection des informations

PDT-STOCK: stockage des informations. Dans la mesure du possible, les données traitées par les utilisateurs doivent être stockées sur des espaces réseau, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur.

6. Sécurisation des imprimantes et copieurs multifonctions

Objectif 12 : sécurisation des copieurs multifonctions. Paramétrer les imprimantes et copieurs multifonctions afin de diminuer leur surface d'attaque.

7. Sécurisation de la téléphonie

Objectif 13 : sécurisation de la téléphonie. Sécuriser la téléphonie pour protéger les utilisateurs contre des attaques malveillantes.

8. Contrôles de conformité

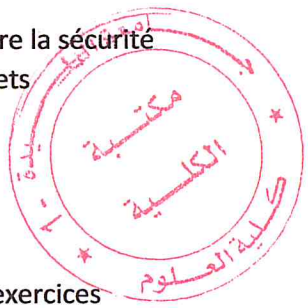
Objectif 13 : contrôles de la conformité des postes de travail. Contrôler régulièrement la conformité des paramétrages de sécurité appliqués aux postes de travail.

PDT-CONF-VERIF : utiliser des outils de vérification automatique de la conformité. Un outil de vérification régulière de la conformité des éléments de configuration des postes de travail doit être mis en place, afin d'éviter une dérive dans le temps de ces éléments de configuration.

9. Sécurité du développement des systèmes

1. Développement des systèmes

Objectif 29 : prise en compte de la sécurité dans le développement des SI. Reconnaître la sécurité comme une fonction essentielle, et la prendre en compte dès la conception des projets.



12. Traitement des incidents

13. Conformité, audit, inspection, contrôle

Objectif 14 : contrôles réguliers. Effectuer des contrôles (audits, inspections) et des exercices réguliers de façon à mesurer les progrès accomplis et corriger les manquements.

14. Plan de continuité

L'entité doit définir un plan de continuité et les procédures correspondantes. Ce plan doit permettre, dans un premier temps, de maintenir en mode dégradé les activités critiques, puis de récupérer et de restaurer toutes les fonctionnalités du système d'information.