République Algérienne Démocratique et Populaire
Ministère de l'enseignement supérieur
et de la recherche scientifique

Université du 08 mai 45, Guelma
Faculté des sciences économiques et commerciales
et sciences de gestion
Département des sciences de gestion

Mémoire présenté pour l'obtention
du diplôme de Master en sciences de gestion
Option: Techniques d'information et de communication
dans l'entreprise

Thème

Etablir une politique de sécurité du système d'information dans l'université 8 mai 1945 Guelma

Réalisé par :
Mlle. BOUKHALFA Fatima Zahra
Mme. HAFFERSSAS Khadîdja

Sous la direction de :
Mr. BENABDALLAH Ahcene youcef
Mr NOUAR Fayçal

Année universitaire 2014-2015

Remerciements

Nous tenons à remercier tout d'abord notre directeur de recherches, Monsieur NOUAR Fayçal, et surtout Monsieur Ben Abdallah youcef pour son encadrement, ses conseils avisés, et la liberté qu'il nous a accordée tout au long de notre recherche. Nous lui exprimons toute notre gratitude.

Nous tenons à remercier également les membres de jury de ce mémoire : Messieurs Djabar Yacine et Douha Djamel, d'avoir accepté de prendre le temps d'évaluer ce travail et de participer à sa soutenance.

Merci à Mr. Chelaghmia Abdel Malek et Mme. Sedraoui Soumya pour leur générosité et leurs conseils éclairés qui nous ont été d'une aide très précieuse.

Merci à Mr. Chouarbia Abdelhafid et Mr.Boussena Abdelhafid pour leurs inlassables encouragements, nous les remercions du fond du coeur.

Merci à tous les enseignants du département de gestion dont les remarques et les conseils ont enrichi nos travaux, sans parler de leur soutien moral durant les moments de doute.

Que tous ceux qui nous ont aidés de près ou de loin dans la réalisation de ce modeste travail trouvent ici l'expression de notre sincère gratitude.

Fatima zahra /khadidja

A :

A l'homme de ma vie,
Mon exemple éternel,
Mon soutien moral et source de joie,
De bonheur, et de tous mes efforts,
Celui qui s'est toujours sacrifié pour me voir réussir,
À toi mon père… ***Amar***

A la lumière de mes jours,
La flamme de mon cœur,
Ma vie et mon bonheur,
A maman ***fadila*** *que j'adore.*
Que DIEU te bénisse dans son vaste Paradis…

Fatima zahra

A très chère Mère : Zahra,

C'est un moment de plaisir de vous dédié cet œuvre, vous qui ravivez dans mon esprit un sentiment profond d'une vie sur et correcte, suivi tant par tes chaleureuses bénédictions

A mon très chère Père : Mahmoud Tayeb

En signe d'amour, de reconnaissance et de gratitude pour ce dévouement et les sacrifices dont vous avez fait toujours prévus à mon égard

'Que nulle dédicace ne puisse exprimer ce que je leurs dois, pour leur bienveillance, leur affection et leur soutien… Trésors de bonté, de générosité et de tendresse, en témoignage de mon profond amour et ma grande reconnaissance « Que Dieu vous garde »'.

A Mon Mari : Yazid
Pour son précieux soutien, pour sa patience, pour avoir cru en moi, pour son sourire réconfortant.

A mon petit cœur :JAD Mouhemed Amine
que dieu te protège et te garde pour moi.

A ma belle-sœur :Fatima
Je vous remercie pour votre encouragement

A ma très chère Cousine : TIMA
T'occupes une place particulière dans mon cœur. Je te souhaite un avenir radieux, plein de Bonheur et de succès.

A ma collègue de ce travail ZAHRA.

A toute ma famille et la famille oumedour.

Enfin, je tiens à remercier tous ceux qui ont prêté main forte dans l'élaboration de ce travail spécialement Radouane, Menel.

Khadidja

Table des matières :

Introduction Générale :

Chapitre 1:

Principes de sécurité du système d'information

Chapitre 2 :

Méthodes et Normes de Sécurité

Chapitre 03 :

La Normes ISO 27002

Chapitre 04 :

Audit du SSI de l'université 8 Mai 1945

Chapitre 5 :

Les Règles de Sécurité pour L'Université de Guelma

Chapitre 06 :

Gestion des Incidents et plan de continuité de travail du SSI

Chapitre 07 :

La charte du système d'information de l'université

Conclusion Générale

Liste des figures :

Liste des tableaux :

Introduction Générale

Les évolutions récentes et rapides de l'informatique ont contribué à l'accélération des échanges d'informations qui se trouvent généralement sous trois formes : données, connaissances et messages. On a l'habitude de désigner par « système d'information » un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, classifier, traiter et diffuser l'information sur un environnement donné.

Toutes les informations détenues et traitées alors sont exposées à des menaces, dont 80 % des cas, ce sont les maladresses internes (volontaires ou non) ou l'absence de sauvegardes fiables qui sont à l'origine de la perte ou de la de striction d'informations sensibles. Les 20 % restants sont imputables à des actes externes mal intentionnés, d'événement naturel (inondation ou incendie), et sont exposées à des vulnérabilités inhérentes à leur utilisation.

Les menaces contre le système d'information entrent dans l'une des catégories suivantes : atteinte à la disponibilité des systèmes et des données, destruction de données, corruption ou falsification de données, vol ou espionnage de données, usage illicite d'un système ou d'un réseau, usage d'un système compromis pour attaquer d'autres cibles.

Véritable point névralgique, le système d'information est souvent la proie de multiples attaques qui menacent l'activité d'établissement ou d'entreprise et requièrent la mise en place d'une politique interne de sécurité.

La sécurité des systèmes d'information et de communication dans l'enseignement supérieur est un problème complexe aux dimensions légales, éthiques, sociales, organisationnelles et techniques. Pour atteindre un niveau de sécurité satisfaisant, une étape primordiale consiste à spécifier simultanément les propriétés désirées et d'établir un cadre réglementaire pour assurer la protection.

Dans ce contexte, l'université 8 Mai 1945 Guelma possède un système d'information important et sensible, gérant une diversité de ses services (scolarité, messagerie, intranet, ..), sur 04 sites géographiquement différents, caractérisé par une absence totale de notion de

sécurité de ce système, pour cela il nous a été confié d'établir une politique de sécurité de haut niveau.

L'objectif de ce travail consiste à établir une politique de sécurité du système d'information de l'université de Guelma afin d'assurer une bonne protection de toute sorte d'information circulant dans ce systèmes, minimiser les risques et d'assurer une continuité de service en cas de problèmes ou d'incidents, en se basant sur le domaine organisationnelle, technique environnemental et humaine.

Par le biais d'un audit, et en faisant appel à une norme de sécurité, pour détecter les failles et les vulnérabilités en amont d'un coté et d'obtenir un aperçu du niveau de sécurité souhaité de l'autre coté, afin d'établir une politique de sécurité adéquate à cet établissement qui se constitue généralement d'un ensemble de règles que nous devons suivre.

Après cette introduction, ce manuscrit est organisé comme suit :

- ✓ Le **premier chapitre**, présente les notions de base de la sécurité d'information, ses critères fondamentaux, ses domaines d'application et ses différentes facettes, la une typologie des risques informatiques ainsi que les quatre étapes du Systèmes de Management de la Sécurité.
- ✓ Le **deuxième chapitre** illustre l'ensemble des méthodes et des normes de sécurité utilisées pour arriver à sécurité une entreprise voire établissement.
- ✓ Le **troisième chapitre** détaille la norme ISO 27002 qui répond à nos besoins, d'où on présente sa définition son historique puis on passe à détailler l'ensemble de ses chapitres en démontrant son évolution et on termine par lister ses avantages.
- ✓ Le **quatrième chapitre** présente l'opération d'audit sur la sécurité des systèmes d'information effectuée au sein de l'université 8 mai 1945 Guelma.
- ✓ Le **cinquième chapitre** propose les règles réparties par thème à mettre en œuvre pour pallier aux insuffisances et afin d'atteindre une bonne politique de sécurité de système information.
- ✓ Le **sixième chapitre** présent un plan d'action pour la gestion des problèmes qui touchent la sécurité de systèmes d'information de l'université, le premier s'articule autour de la gestion d'incidents au niveau de ce système, par contre le deuxième gère la continuité du travail de ce même système.
- ✓ Le **dernier chapitre** présent une charte destinée à l'ensemble du personnel et d'utilisateurs du système d'information de l'université, et on termine ce mémoire par une conclusion et quelques perspectives.

Conclusion Générale

De nos jours, l'université reconnait que ces informations, essentielles à ses activités d'administration, d'enseignement ou de recherche, doivent faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate, et ce, tout au long de son cycle de vie.

Etant consciente de leur importance, l'administration de l'université a émis le souhait d'établir une politique de sécurité de son systèmes d'information. Pour cela l'objectif de notre c'était la proposition d'une politique de sécurité

En adoptant la méthodologie du Système de Gestion de la Sécurité de l'Information (ISMS) selon la norme ISO 27001 ,en basant sur la première étape (Plan) , nous avons lancé une opération d'audit sur le contexte de PSSI, ou nous avons adopté une approche qui consiste à mesurer le niveau de maturité en se basant sur un questionnaire à base de la norme ISO 27002 .

Les résultats d'audit confirment l'absence totale d'une politique de sécurité de cet établissement à part quelques initiatives personnelles, ce qui nous a conduit à suggérer un ensemble de règles réparties par thème à mettre en œuvre pour pallier aux insuffisances constatées précédemment, sur le domaine organisationnel, environnemental, technique et humain, et proposer une charte du bon usage du système d'information.

Vu l'importance et la sensibilité de ce thème, on a eu beaucoup de difficultés pour arriver à avoir l'information exacte, citant à titre d'exemple le nombre réel des ordinateurs (poste de travail), et routeurs, les algorithmes utilisés dans le routage,…etc., plus la confidentialité de certaines informations.

Nous souhaitons que cette politique soit appliquer et suivi par le staff technique et administratif de l'université de Guelma afin d'élever son niveau de protection, et éviter les incidents connus auparavant, ce qui rend son système plus stabilité.

Parmi nos perspectives, l'enrichissement de ces règles, et le suivi, pour arriver à mettre en place une bonne politique de sécurité qui s'étale généralement sur trois (3) années consécutives selon la recommandation internationale.

Chapitre 1 : Principes de sécurité du système d'information

Introduction

Nous présentons dans ce premier chapitre, les notions de base de la sécurité d'information, ses critères fondamentaux, ses domaines d'application et ses différentes facettes, ensuite nous donnons une typologie des risques informatiques ainsi que les quatre étapes du Systèmes de Management de la Sécurité en basant sur la première étape (Plan) qui nous intéresse pour notre étude.

1 Système d'Information et informatique

1.1 Systèmes d'information

L'information se présente sous trois formes: les données, les connaissances et les messages. On a l'habitude de désigner par « système d'information» l'ensemble des moyens techniques et humains qui permet de stocker, de traiter ou de transmettre l'information **[1]**.

1.2 Système informatique

Un système informatique est un ensemble de dispositifs (matériels et logiciels) associés, sur lesquels repose un système d'information. Il est constitué généralement des serveurs, routeurs, pare-feu, commutateurs, imprimantes, médias (câbles, air, etc.), points d'accès, stations de travail, systèmes d'exploitation, applications, bases de données, etc.

2 La Sécurité

2.1 Concept et définition

La sécurité d'une manière générale, est l'état d'une situation présentant le moindre risque, ou l'état d'esprit d'une personne qui se sent tranquille et confiante. Pour un individu ou un groupe ; c'est sentiment (bien ou mal fondé) d'être à l'abri tout danger et risque **[2]**.

La sécurité informatique consiste à assurer que les ressources du système d'information (matériels et/ou logiciels) d'une organisation sont uniquement utilisées dans le cadre ou il est prévu qu'elles le soient **[3]**, comme on peut dire c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles, en anglais Sécurité veut dire "Safety" c.à.d. protection de systèmes informatiques contre les accidents dus à l'environnement et les défauts du système, comme il veut dire aussi Sécurité = "Security " c.à.d. protection des systèmes informatiques contre des actions malveillantes intentionnelles.

2.2 Risque

En général, le risque en termes de sécurité est caractérisé par l'équation suivante :

RISQUE = MENACE * VULNÉRABILITÉ * IMPACT

Pour bien comprendre la notion de risque, il est important de se pencher sur chacune de ses composantes. Tout d'abord **[2]** :

- **la menace :** la source du risque, est l'attaque possible d'un élément dangereux pour les assets. C'est l'agent responsable du risque.
- **la vulnérabilité :** est la caractéristique d'un asset constituant une faiblesse ou une faille au regard de la sécurité. Enfin l'impact représente la conséquence du risque sur l'organisme et ses objectifs. La menace et la vulnérabilité, représentant la cause du risque, peuvent être qualifiées en termes de potentialité.
- **L'impact** peut, quant à lui, être qualifié en termes de niveau de sévérité.

3 Les critères fondamentaux de la sécurité informatique

La notion de sécurité fait référence à la propriété d'un système, d'un service ou d'une entité. Elle s'exprime le plus souvent par les objectifs de sécurité suivants **[4] :**

- la disponibilité (D) ;
- l'intégrité (I) ;
- la confidentialité (C).

Ces objectifs peuvent être compris comme étant des critères de base (dits critères DIC) auxquels s'ajoutent des fonctions de sécurité qui contribuent à confirmer d'une part la véracité, l'authenticité d'une action, entité ou ressource (notion d'authentification), et d'autre part, l'existence d'une action (notion de non-répudiation d'une Transaction, voire d'imputabilité).

3.1 Disponibilité

La disponibilité d'une ressource est relative à la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la capacité d'une ressource à être utilisée (serveur ou réseau par exemple).

Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être accessible par l'ensemble des ayants droit **(**notion d'accessibilité) **[4]**.

3.2 Intégrité

Le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions, services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour contribuer à préserver son intégrité, permettra de la protéger plus ou moins efficacement contre une menace de corruption ou de destruction.

3.3 Confidentialité

Selon le petit Robert : *« La confidentialité est le maintien du secret des informations…»,* Transposée dans le contexte de l'informatique et des réseaux, la notion de confidentialité peut être vue comme la protection des données contre une divulgation non autorisée *;* il existe deux types d'actions complémentaires permettant d'assurer la confidentialité des données :

- limiter et contrôler leur accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire ;
- les rendre inintelligibles en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.

Le chiffrement des données (ou cryptographie) contribue à assurer la confidentialité des données et à augmenter la sécurité des données lors de leur transmission ou de leur stockage. Bien qu'utilisées essentiellement lors de transactions financières et commerciales, les techniques de chiffrement sont relativement permises en œuvre par les internautes de manière courante **[4]**.

3.4 Identification et authentification

Identifier l'auteur présumé d'un tableau signé est une chose, s'assurer que le tableau est authentique en est une autre. Il en est de même en informatique où des procédures d'identification et d'authentification peuvent être mises en œuvre pour contribuer à réaliser des procédures de contrôle d'accès et des mesures de sécurité assurant :

- la confidentialité et l'intégrité des données : seuls les ayants droit identifiés et authentifiés peuvent accéder aux ressources (contrôle d'accès) et les modifier s'ils sont habilités à le faire ;
- la non-répudiation et l'imputabilité : seules les entités identifiées et authentifiées ont pu réaliser une certaine action (preuve de l'origine d'un message ou d'une transaction, preuve de la destination d'un message…). L'identification et l'authentification des ressources et des utilisateurs permettent d'imputer la responsabilité de la réalisation d'une action à une entité.

3.5 Non-répudiation

La non-répudiation est le fait de ne pouvoir nier ou rejeter qu'un événement(action, transaction) a eu lieu. À ce critère de sécurité peuvent être associées les notions d'imputabilité, de traçabilité ou encore parfois d'adaptabilité.

L'imputabilité définit par l'attribution d'une action (un événement) à une entité déterminée (ressource, personne). Elle peut être réalisée par un ensemble de mesures garantissant l'enregistrement fiable d'informations pertinentes par rapport à une entité et à un événement **[4]**.

4 Domaines d'application de la sécurité Informatique

Pour une organisation, toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité d'un système d'information. En fonction de son domaine d'application la sécurité informatique se décline en dans la figure 1.1:

- sécurité physique et environnementale ;
- sécurité de l'exploitation ;
- sécurité logique, sécurité applicative et sécurité de l'information ;
- sécurité des infrastructures informatique et de télécommunication (sécurité des
- réseaux, sécurité Internet et cyber sécurité).

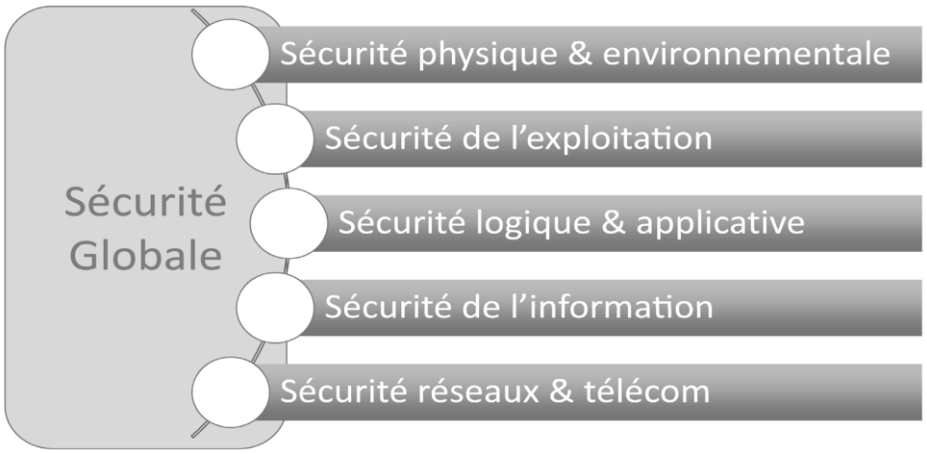


Figure 1.1 : Domaines d'application de la sécurité

4.1 Sécurité physique et environnementale

La sécurité physique et environnementale concerne tous les aspects liés à la maîtrise des systèmes et de l'environnement dans lesquels ils se situent.

Sans vouloir être exhaustif, nous retiendrons que la sécurité physique repose essentiellement sur :

- la protection des sources énergétiques et de la climatisation (alimentation électrique, refroidissement, etc.) ;
- la protection de l'environnement (mesures *ad hoc* notamment pour faire face aux risques d'incendie, d'inondation ou encore de tremblement de terre, pour respecter les contraintes liées à la température, à l'humidité, etc.) ;
- des mesures de gestion et de contrôle des accès physiques aux locaux, équipements et infrastructures (avec entre autres la traçabilité des entrées et une gestion rigoureuse des clés d'accès aux locaux) ;
- l'usage d'équipements qui possèdent un bon degré de sûreté de fonctionnement et de fiabilité ;
- le marquage des matériels pour notamment contribuer à dissuader le vol de matériel et éventuellement le retrouver ;
- le plan de maintenance préventive (tests, etc.) et corrective (pièces de rechange, etc.) des équipements ce qui relève également de la sécurité de l'exploitation des environnements.

4.2 Sécurité de l'exploitation

La sécurité de l'exploitation doit permettre un bon fonctionnement opérationnel des systèmes informatiques. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour.

La sécurité de l'exploitation dépend fortement de son degré d'industrialisation, qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches. Bien que relevant de la responsabilité de l'exploitation, ces conditions concernent très directement la conception et la réalisation des applications elles-mêmes et leur intégration dans un système d'information.

4.3 Sécurité logique, applicative et sécurité de l'information

La sécurité logique fait référence à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes, des services offerts et à la protection des données. Elle s'appuie généralement sur :

- la qualité des développements logiciels et des tests de sécurité ;
- une mise en œuvre adéquate de la cryptographie pour assurer intégrité et confidentialité;
- des procédures de contrôle d'accès logique, d'authentification;
- des procédures de détection de logiciels malveillants, de détection d'intrusions et d'incidents ;
- mais aussi sur un dimensionnement suffisant des ressources, une certaine redondance ainsi que sur des procédures de sauvegarde et de restitution des informations sur des supports fiables éventuellement spécialement protégés et conservés dans des lieux sécurisés pour les applications et données critiques.

4.4 Sécurité des infrastructures de télécommunication

La sécurité des télécommunications consiste à offrir à l'utilisateur final et aux applications communicantes, une connectivité fiable de « bout en bout ». Cela passe par la réalisation d'une infrastructure réseau sécurisée au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler) et cela s'appuie sur des mesures architecturales adaptées, l'usage de plates-formes matérielles et logicielles sécurisées et une gestion de réseau de qualité **[5]**.

La sécurité des télécommunications ne peut à elle seule garantir la sécurité des informations. Elle ne constitue qu'un maillon de la chaîne sécuritaire car il est également impératif de sécuriser l'infrastructure informatique dans laquelle s'exécutent les programmes. Pris au sens large, cela comprend la sécurité physique et environnementale des systèmes (poste de travail de l'utilisateur, serveur ou système d'information, (figure 1.2).

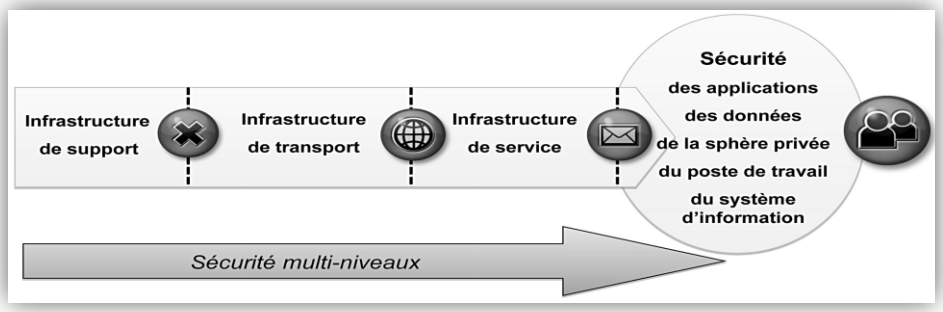


Figure 1.2 : Sécurité des infrastructures de télécommunication

5 Classification des risques

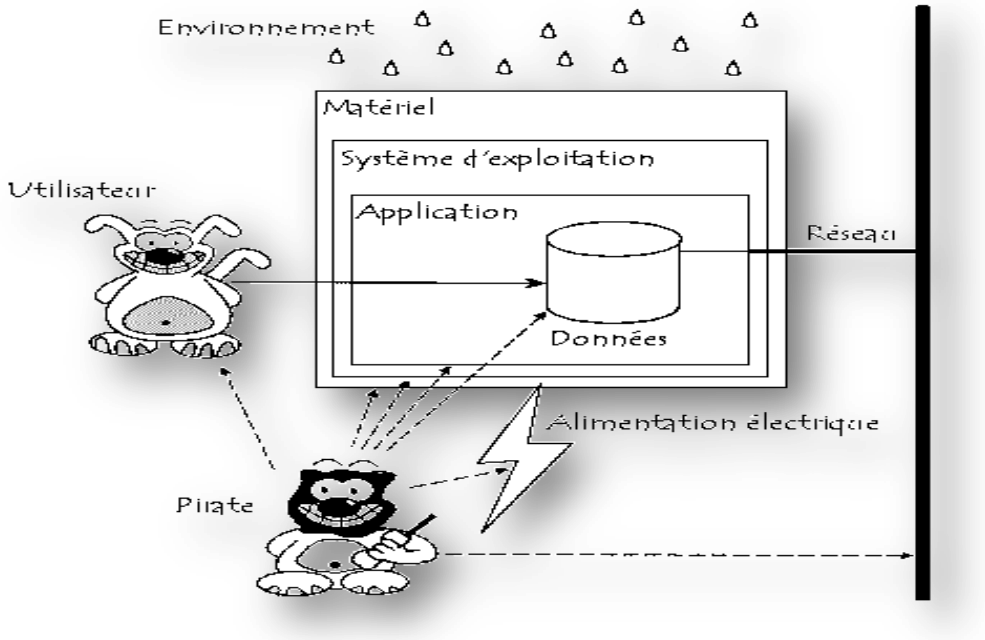


Figure 1.3 : Les risques informatiques **[8]**

5.1 Les risques Humains

Les risques humains sont les plus importants, ils concernent les utilisateurs mais également les informaticiens.

- **Malveillances :** Certains utilisateurs peuvent volontairement mettre en danger le système d'information en y introduisant en connaissance de causes des virus, ou en introduisant volontairement de mauvaises informations dans une base de données.
- **Maladresse :** Comme en toute activité les humains commettent des erreurs, ils leur arrivent donc plus ou moins fréquemment d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes.

- **Inconscience :** De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils encourent aux systèmes qu'ils utilisent, et introduisent souvent des programmes malveillants sana le savoir.

5.2 Les risques Techniques

- **Programmes malveillants :** C'est un logiciel développé dans le but de nuire à un système informatique. Voici les principaux types de programmes malveillants :
- **Le virus** : Programme se dupliquant sur d'autres ordinateurs.
- **Le Cheval de Troie** : Programme à apparence légitime qui exécute des routines nuisibles sans l'autorisation de l'utilisateur.
- **Accidents :** il s'agit là d'un évènement perturbant les flux de données en l'absence de dommages aux équipements (panne, incendie, dégâts des eaux d'un serveur ou centre informatique,..).
- **Erreurs :** que ce soit une erreur de conception, de programmation de paramétrage ou de manipulation de données ou de leurs supports, l'erreur désigne les préjudices consécutifs à une intervention humaine dans le processus de traitement automatisé des données.

5.3 Technique d'attaques par messagerie

En dehors de nombreux programmes malveillants qui se propagent par la messagerie électronique, il existe des attaques spécifiques tels que :

- **Le Pourriel (*Spam*)** : Un courrier électronique non sollicité, la plus part du temps de la publicité. Ils encombrent le réseau.
- **Hameçonnage** : un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles.

5.4 Attaques sur le réseau

Les principales techniques d'attaques sur le réseau sont :

- ***Le Sniffing*** : technique permettant de récupérer toutes informations transitant sur le réseau.
- Elle est généralement utilisée pour récupérer les mots de passe des applications qui ne chiffrent pas leurs communications.
- **La Mystification *(Spoofing*)** : technique consistant à prendre l'identité d'une autre personne ou d'une autre machine. Elle est généralement utilisée pour récupérer des informations sensibles.

5.5 Attaques sur les mots de passe

Les attaques sur les mots de passe peuvent consister à fairede nombreux essais jusqu'à trouver le bon mot de passe.

Dans ce cadre, notons les deux méthodes suivantes :

- **L'attaque par dictionnaire** : le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants.
- **L'attaque par force brute** : toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution (par exemple de "aaaaaa "jusqu'à "zzzzzz" pour un mot de passe composé strictement de six caractères alphabétiques) **[7]**.

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

6.1 Les systèmes de management

La norme ISO 9000 définit le système de management comme : *un système permettant d'établir une politique, des objectifs et 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 1.4 ci-dessous.

Figure 1.4 : Vue d'un système de management

Un système de management se caractérise par un engagement de l'ensemble des collaborateurs de l'organisme ; quel que soit le périmètre du système sur l'activité de l'organisme, il nécessite l'implication de tous les métiers. A cette approche transversale doit s'associer une approche verticale. L'ensemble de la hiérarchie de l'organisme, de la direction jusqu'aux parties intéressées, c'est-à-dire les fournisseurs, partenaires et actionnaires doivent être engagés dans la mise en œuvre du système. Une autre caractéristique des systèmes de management est la formalisation des politiques et procédures de l'organisme afin de pouvoir être audité.

Ces engagements ont un coût en ressources matérielles, humaines et financières. Comment justifier cet investissement ? Les systèmes de management s'appuient sur des guides de bonnes pratiques, mécanismes d'amélioration continue favorisant la capitalisation sur les retours d'expérience, ce qui a pour effet d'accroitre la fiabilité. En outre, l'audit du système de management

par un cabinet d'audit indépendant permet d'établir une relation de confiance entre le client et le fournisseur.

Le fonctionnement du système de management se fait selon le modèle PDCA de l'anglais Plan, Do, Check, Act, en français planifier, faire, contrôler et corriger. Ces quatre phases sont illustrées dans la figure 1.5 ci-dessous **[9]**.

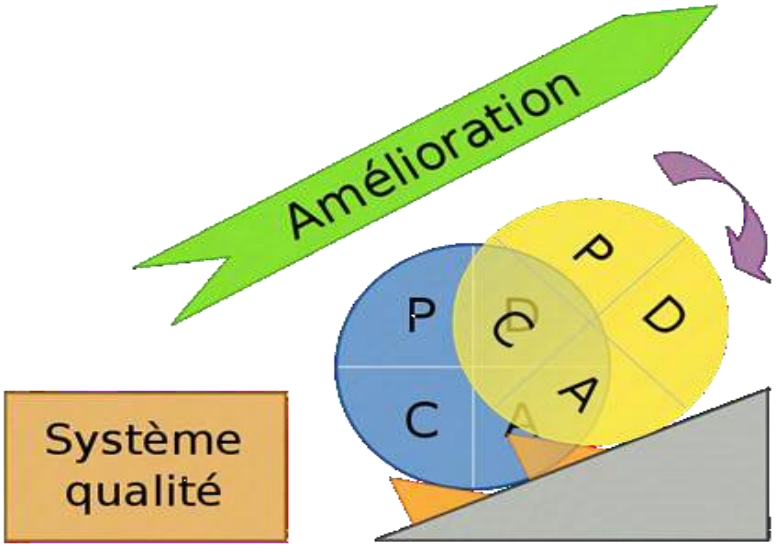


Figure 1.5: Roues de Deming (PDCA)

- **Plan** : dire ce que l'on va réaliser dans un domaine particulier.
- **Do** : faire ce qui a été annoncé.
- **Check** : vérifier les écarts entre les phases « plan » et «do ».
- **Act** : ajuster les écarts constatés de la phase « check ».

Une fois que les objectifs fixés par le management sont atteints, il faut s'y tenir dans la durée. La flèche sur la roue Deming, montre qu'un nouveau cycle du processus du système de management doit être entrepris pour y parvenir. Notons que le modèle PDCA s'applique au système de management dans son ensemble ainsi qu'à chacun de ses processus.

On retrouve les systèmes de management dans des secteurs d'activités aussi variés que la santé et la sécurité du travail avec la norme OHSAS 18001, l'environnement avec la norme ISO 14001, les services informatiques avec le référentiel ISO/CEI 20000, la sécurité alimentaire avec la norme ISO 22000, la qualité avec la norme ISO 9001 ou encore la sécurité de l'information avec la norme ISO/CEI 27001 que nous allons traiter dans les points suivants.

6.2 Sécurité de l'information

Dans le SMSI, l'information n'est pas restreinte systèmes informatiques.

L'information est à prendre au sens large du terme. Elle doit être étudiée sous toutes ses formes indépendamment de son support, humain, papier, logiciel, etc. Le terme sécurité doit être compris comme l'ensemble des moyens déployés pour se protéger contre les actes de malveillance.

6.2.1 Phase « PLAN » du PDCA

La phase « Plan » du PDCA consiste à fixer les objectifs du SMSI en suivant quatre grandes étapes, la politique et le périmètre du SMSI, l'appréciation des risques, le traitement des risques décidé en tenant en compte des risques résiduels et la sélection des mesures de sécurité présentées dans le SoA (Statement of Applicability). La figure 1.6 ci-dessous présente, une vue du déroulement de la phase Plan.

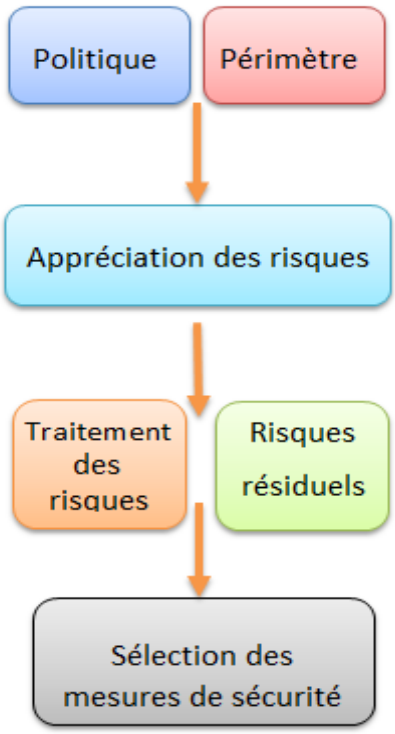


Figure 1.6 : Etapes de la phase Plan du PDCA

6.2.1.1 Politique et périmètre du SMSI

La première étape consiste à définir la politique et le périmètre du SMSI. La politique est là pour préciser le niveau de sécurité qui sera appliqué au sein du périmètre du SMSI. La norme ne fixe pas d'exigences sur le périmètre, il peut être restreint ou couvrir l'ensemble des activités de

l'organisme. L'objectif est d'y inclure les activités pour lesquelles les parties prenantes exigent un certain niveau de confiance.

6.2.1.2 Appréciation des risques

La deuxième étape concerne un des points les plus importants de l'ISO/CEI27001, l'appréciation des risques. Le problème de l'appréciation des risques n'est pas nouveau et est traité par de nombreuses méthodes développées dans différents secteurs privés, académiques et agences gouvernementales. Certaines méthodes sont très répandues dans les organismes. En France, les plus connues sont EBIOS et MEHARI, aux Etats-Unis, OCTAVE. L'ISO/CEI propose aussi une méthode, la norme ISO/CEI 27005, mais ne l'impose pas. L'ISO/CEI 27001 ne fait que fixer un cahier des charges spécifiant chacune des étapes clefs de l'appréciation des risques. L'organisme a le libre choix, de développer sa propre méthode en suivant les objectifs fixés par l'ISO/CEI 27001 ou d'en appliquer une déjà éprouvée.

Dans les points suivants nous détaillons le processus d'appréciation des risques.

6.2.1.3 Processus d'appréciation des risques

Le processus d'appréciation des risques se déroule en sept étapes, illustrées dans figure 1.7 ci-dessous :

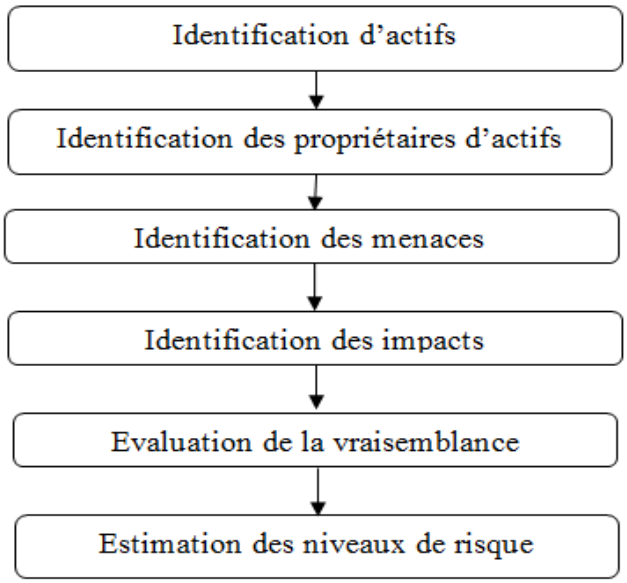


Figure 1.7 : Processus d'appréciation des risques

- **La première étape** : consiste dresser une liste de tous les actifs qui ont une importance en matière d'information au sein du SMSI. On distingue généralement six catégories d'actifs.
  - Matériel, pour tous les équipements réseau et système.
  - Physique, pour les bureaux, lieux de production, de livraisons.

- Logiciel, pour les bases de données, fichiers, les systèmes d'exploitation.
- Humain, pour tous les collaborateurs de l'organisme.
- Documents, pour les documents papier, manuels d'utilisation.
- Immatériel, pour le savoir-faire de l'organisme.

- **La deuxième étape** : vise à attribuer pour chaque actif d'information un Propriétaire.
  La norme définit le propriétaire comme étant la personne qui connaît le mieux la valeur et les conséquences d'une compromission en termes de disponibilité, d'intégrité et de confidentialité de l'actif.
- **La troisième étape :** est l'identification des vulnérabilités des actifs recensés. La vulnérabilité est la propriété intrinsèque du bien qui l'expose aux menaces. A titre d'exemple, un ordinateur portable est vulnérable au vol mais sa vulnérabilité n'est pas le vol mais sa portabilité. Dans ce cas l'identification de la vulnérabilité est la portabilité.
- **La quatrième étape** : est l'identification des menaces qui pèsent sur les actifs d'information précédemment recensés. Si l'on reprend l'exemple de l'ordinateur portable, la menace est dans ce cas le vol.
- **La cinquième étape :** vise à évaluer l'impact d'une perte de la confidentialité, de la disponibilité ou de l'intégrité sur les actifs. Pour mesurer cet impact on peut par exemple utiliser une matrice des risques, la norme n'impose aucun critère de mesure.
- **La sixième étape :** demande d'évaluer la vraisemblance des précédentes étapes du processus en plaçant dans leur contexte les actifs. Il s'agit par exemple de considérer les mesures de sécurité déjà en vigueur dans l'organisme. Si l'ordinateur portable possède une clef d'authentification, un cryptage de ses données ou un accès VPN pour travailler, alors la vraisemblance d'observer un impact sur la confidentialité, la disponibilité ou l'intégrité de ses données est limitée.
- **La septième étape** : consiste à attribuer une note finale reflétant les risques pour chacun des actifs d'information. La norme n'impose aucune formule, on peut par exemple utiliser un code couleur (rouge pour un niveau de risque très élevé, orange pour moyen et vert pour faible).

6.2.1.4 Traitement des risques

La troisième étape concerne le choix du traitement des risques. L'ISO/CEI 27001a identifié quatre traitements possibles du risque, l'acceptation, l'évitement, le transfert et la réduction.

- « Accepter » le risque revient à ne déployer aucune mesure de sécurité autre que celles déjà en place. Cette décision peut être justifiée si le vol de données dans un cas précis n'a pas d'impact sur l'organisme.
- « Eviter » le risque consiste à supprimer par exemple l'activité ou le matériel offrant un risque.
- « Transférer » un risque par souscription d'une assurance ou par sous-traitance. Ces moyens de transfert du risque sont souvent employés quand d'organisme ne peut ou ne souhaite pas mettre en place les mesures de sécurité qui permettraient de le réduire.
- « Réduire » le risque consiste à prendre des mesures techniques et organisationnelles pour ramener à un niveau acceptable le risque. C'est le traitement le plus courant.

Il existe d'autres traitements du risque possibles mais pour être en conformité avec la norme, il faut en priorité considérer ceux que nous venons de citer.

Après avoir sélectionné le traitement et mis en place les mesures de sécurité, un risque peut persister. Il convient de traiter ce risque comme les autres c'est-à-dire, l'accepter, l'éviter, le transférer ou le réduire **[9]**.

6.2.1.5 Sélection des mesures de sécurité

L'étape 4 est la dernière étape de la phase « Plan » du PDCA, elle consiste à sélectionner les mesures de sécurité. La norme ISO/CEI 27001 propose dans son annexe A, 133 mesures de sécurité réparties sur onze chapitres. A ce stade, le travail consiste à dresser un tableau, appelé SoA (Statement of Applicability) dans lequel figurent les 133 mesures qu'il faut déclarer applicables ou non applicables, pour réduire les risques du SMSI. Notons que les 133 mesures proposées par l'ISO/CEI 27001 répertorient presque tout ce qui peut être entrepris en matière de sécurité de l'information cependant, cette liste ne comporte pas d'exemples ni d'explications sur le déploiement des mesures à entreprendre. L'ISO/CEI 27002répond en partie à ce besoin en fournissant une série de préconisations et d'exemples techniques et organisationnels qui couvrent la liste de l'ISO/CEI27001.

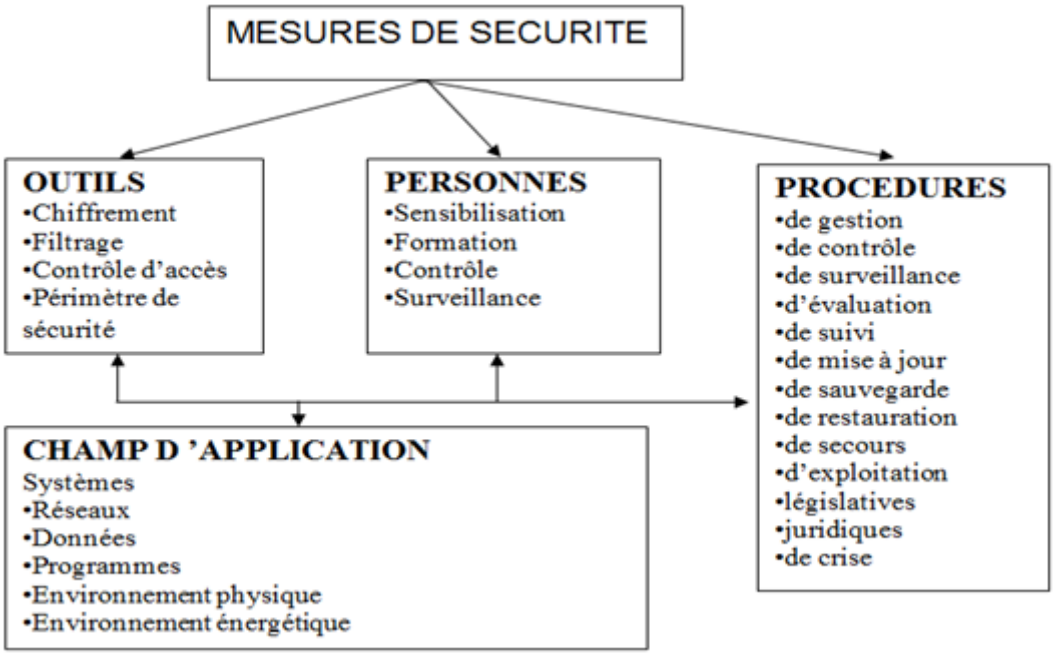


Figure 1.8 : Complémentarité des procédures, outils et personnes

Conclusion

Au cours de ce chapitre, nous avons présenté des généralités sur la sécurité de l'information, nous avons cité également ses différents domaines d'application .le prochain chapitre s'articulera sur les méthodes et les normes du système de la sécurité de l'information.

Chapitre 2 : Méthodes et Normes de Sécurité

Introduction

Dans ce chapitre, nous illustrons les méthodes et les normes de sécurité utilisées Pour protéger un système d'information, dans la première partie l'ensemble des méthodes classées en deux approches : approche orientées de gestion et approches orientées processus. Dans la deuxième partie nous présentons la famille des normes de sécurité ISO 2700x.

1 Les Méthodes de sécurité

Les méthodes de sécurité sont classées en deux approches, et chaque approche comporte plusieurs méthodes.

1.1 Approches orientées gestion de risques

Dans la littérature, plusieurs méthodes de gestion de risques informatiques sont Définies **[10]**.

Nous présentons les deux méthodes utilisées en France : EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) et MEHARI (Méthode Harmonisée d'Analyse de Risques). Ces méthodes séparent les actifs d'une organisation des vulnérabilités techniques et des menaces pour en déduire les risques potentiels afin de proposer des mesures de sécurité à appliquer **[11**].

1.1.1 EBIOS

La méthode EBIOS **[12]** définie par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) fournit un guide méthodologique pour identifier les besoins de sécurité d'un système d'information existant ou à développer. Elle permet :

1) d'identifier les biens et services à protéger,
2) d'analyser les conséquences d'incidents sur ces biens et services, et,
3) d'analyser parallèlement les vulnérabilités des architectures techniques pour choisir les objectifs de sécurité appropriés pour minimiser les risques **[11]**.

EBIOS, composée de cinq étapes de base, met l'accent sur l'analyse des risques
(Figure 2.1) :

1. Etude de contexte : cette étape a pour objectif d'identifier globalement la cible de sécurité et de la situer dans son environnement. Les contraintes imposées à la cible de sécurité sont identifiées.
2. Expression des besoins en sécurité : une liste des besoins fonctionnels (des besoins auxquels doit répondre la solution proposée et indépendants de toute solution technique), nécessaires pour assurer la sécurité de la cible est créée. Ce besoin de sécurité s'exprime selon différentes propriétés de sécurité telle que la disponibilité, l'intégrité et la confidentialité.
3. Etude des menaces : l'analyse des menaces contribue à l'appréciation des risques. Elle a pour objectif la détermination des menaces pesant sur la solution. Les menaces mises en évidence au travers de cette étape sont spécifiques à la cible de sécurité et leur caractérisation est dépendante des besoins fonctionnels.
4. Identification des objectifs de sécurité : cette étape consiste à analyser l'importance de l'impact des menaces sur les besoins fonctionnels. Une graduation des risques est établie permettant l'élaboration des objectifs de sécurité que le système doit satisfaire pour qu'il fonctionne de manière sûre.
5. Détermination des exigences de sécurité : à partir des objectifs de sécurité, une liste d'exigences de sécurité est produite. Ces exigences de sécurité spécifient de manière précise des fonctionnalités de sécurité nécessaires pour couvrir tous les objectifs de sécurité.

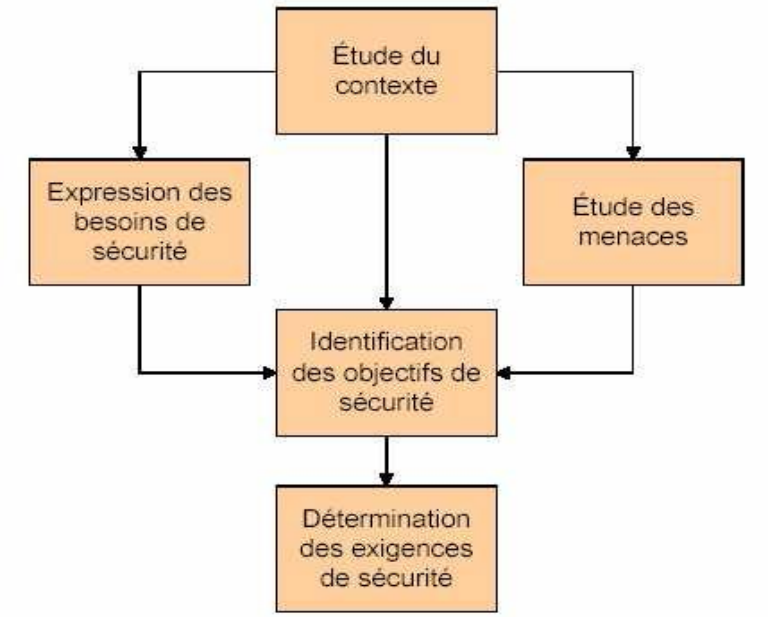


Figure 2.1 : Les étapes de la méthode EBIOS

1.1.2 MEHARI

MEHARI est la toute dernière méthode produite par le CLUSIF (Club de la Sécurité de l'information Français).sa réalisation découle directement de ses consœurs MARION et MELISA. MARION est une méthode d'audit visant à évaluer le niveau de sécurité informatique d'une entreprise, tandis que MELISA est une méthode d'analyse de risques en fonction de l'évaluation des vulnérabilités. La première version de MEHARI fut proposée en 1996, et la plus récente version date de 2007.

La méthode MEHARI **[13]** a été conçue par le CLUSIF pour les grandes entreprises et organismes. Elle prévoit la démarche de sécurité à deux niveaux : stratégique (lié au métier de l'entreprise) et opérationnel. Cette architecture à deux niveaux est bien adaptée pour des grands groupes ; il n'existe pas une version allégée de la méthode orientée petites et moyennes entreprises.

La méthode MEHARI répond à quatre objectifs majeurs :

- Analyser les enjeux majeurs : MEHARI définit l'analyse des enjeux par « *que peut-on redouter et, si cela devrait arriver, serait-ce grave ?* »,
- Etudier les vulnérabilités,
- Réduire la gravité des risques,
- Piloter la sécurité de l'information.

MEHARI version 2007, conçue pour être utilisée dans des contextes d'entreprises différents, est composée de cinq étapes :

- Définition des objectifs et du périmètre et, qui valide les métriques de sécurité,
- Analyse des enjeux qui permet de classifier les actifs de l'entreprise ce qui permet de ne retenir que les risques pesant sur les actifs essentiels,
- Diagnostic des vulnérabilités permettant d'identifier, d'évaluer et de pondérer les menaces entre ceux acceptables et ceux inacceptables,
- Recherche des mesures de sécurité. Dans MEHARI, les mesures de sécurité sont choisies en fonction de leur efficacité et robustesse en regard de la gravité des scénarios de sinistres pour l'entreprise. Quatre niveaux de gravité de sinistre de dysfonctionnement sont distingués (4 : Vital, 3 : Très grave, 2 : Important, 1 : Non significatif) afin d'élaborer les mesures de sécurité. Ces dysfonctionnements peuvent arriver à cause d'absence de confidentialité, intégrité ou disponibilité des ressources et des données.

- Planification et pilotage des chantiers à mener et des résultats obtenus.

MEHARI se compose d'un guide et d'exemples d'utilisation de la méthode.

1.2 Approches orientées processus

1.2.1 ITIL (IT Infrastructure Library)

Parallèlement à ISO 27000 pour la gestion de la sécurité, ITIL (IT Infrastructure Library), s'intéresse aux TI de manière plus générale [14]. ITIL a été développé comme un code de bonnes pratiques pour le management des processus informatiques.

Actuellement en version 3 (Figure 2.2), ITIL est une collection de livres qui recense, synthétise et détaille les meilleures pratiques pour une direction informatique dont l'objectif est d'être le fournisseur de Services basés sur l'informatique au sein de l'organisation plutôt que le traditionnel fournisseur de ressources techniques informatiques [15].

Figure 2.2 : L'architecture ITIL[15]

ITIL fournit un module pour la gestion de la sécurité (*ITIL Security Management process*) basé sur ISO 17799. La démarche générale suit la roue de Deming .À partir de la section sécurité de la SLA (Service Level Agreement - accord entre le fournisseur et le client), la première étape est la planification qui consiste à définir la politique de sécurité ainsi que les OLA (Operational Level Agreement - convention interne au fournisseur) par rapport à l'estimation des risques métier. Cette phase reprend largement la norme ISO 17799pour sélectionner les mesures de sécurité à prendre en compte. Pendant la phase d'implémentation,

les mesures sont implémentées sous la forme de procédures opérationnelles et l'utilisation d'outils de sécurité. La phase suivante évalue la conformité des mesures de sécurité par rapport aux politiques et aux SLA. Enfin, la phase de maintenance améliore la sécurité. Tous ces processus sont vérifiés par un processus de contrôle. Enfin, la gestion de la sécurité est associée aux autres processus ITIL comme la gestion des incidents, des problèmes ou des changements **[16]**.

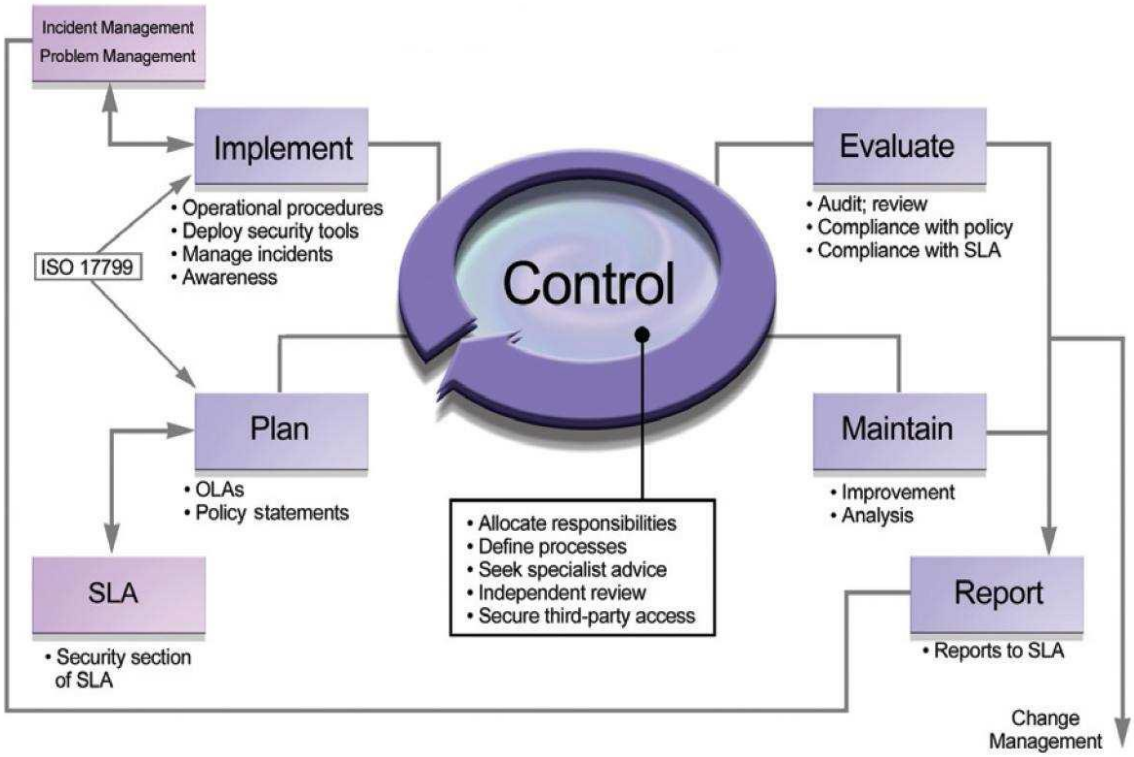


Figure 2.3 : La démarche ITIL

1.2.2 COBIT

D'un autre côté, COBIT (Control Objectives for Business &Related Technology)**[17]** est une méthode pour les gestionnaires qui ont besoin de peser les risques (sécurité, fiabilité, conformité) et de contrôler les investissements dans un environnement des TI qui est peu prévisible. Ainsi, COBIT est un référentiel pour la gouvernance et l'audit des Systèmes d'Information développé par l'ISACA (Information System Audit & Control Association).COBIT adopte une approche orientée processus : tout système informatique est décomposée en 34 processus regroupés en 4 domaines **[16]**.

Le cadre conceptuel de COBIT s'articule autour de trois axes : les processus TI, les critères d'information et les ressources TI (Figure 13).

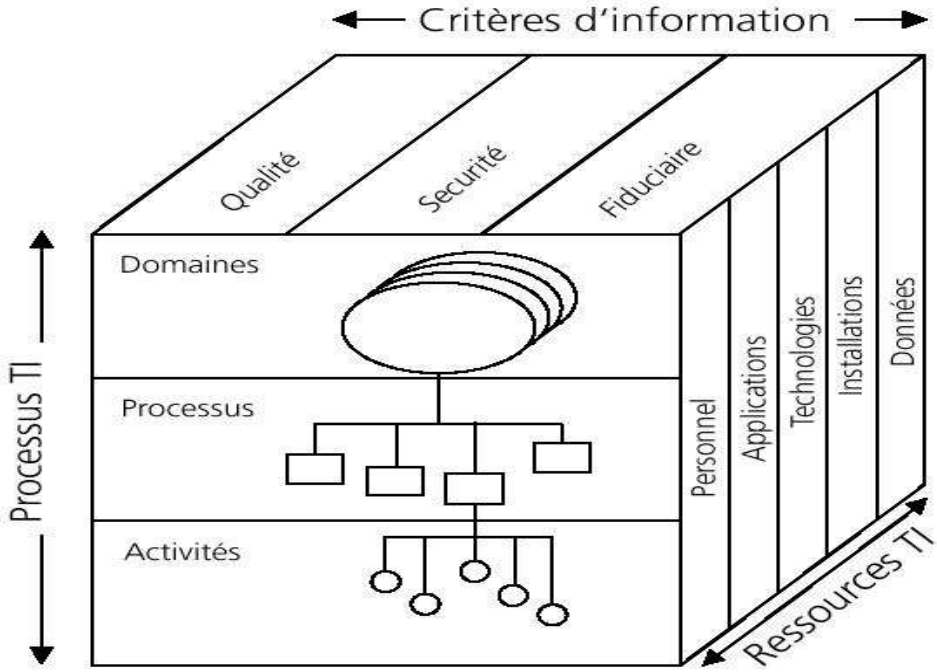


Figure 2.4: Le cube CobiT

1.2.3 CMMI

CMMI (Capability Maturity Model Integration) **[18]** est une approche d'amélioration de processus qui fournit aux organisations les éléments essentiels des processus efficaces. CMMI peut être utilisé pour assurer l'amélioration des processus au sein d'un projet, d'une division, ou de l'organisation en entier. Ceci en permettant l'intégration des fonctionnalités distinctes, en positionnant les objectifs de l'amélioration de processus et en fournissant un point de référence pour l'évaluation des processus actuels.

CMMI est un modèle d'évaluation du niveau de maturité d'une organisation en matière de développements informatiques. CMMI est basé sur le modèle CMM (Capability Maturity Model) **[19]** qui aborde plusieurs cibles. Le SA-CMM (Software Acquisition CMM **[20]**), le People-CMM (pour la gestion des ressources humaines **[21]**) et, le SECMM (System Engineering CMM **[22]**). En 2001, tous ces modèles ont été regroupés dans un seul cadre conceptuel qui est le CMMI. Ainsi, le CMMI reprend l'essentiel des notions du CMM en élargissant son périmètre et propose un référentiel des meilleures pratiques en matière de développement logiciel.

Le CMMI a pour objectif d'encourager les organisations à mettre leurs processus sous contrôle, à les améliorer de façon continue et d'évaluer leur niveau de maturité sur l'échelle de cinq niveaux de maturité proposée :

- Initial (*Initial*)

Les facteurs de réussite des projets ne sont pas identifiés, la réussite ne peut donc être répétée.

- Géré (*Managed*)

Les projets sont pilotés individuellement et leurs succès sont répétables.

- Défini (*Defined*)

Les processus de pilotage des projets sont mis en place au niveau de l'organisation par l'intermédiaire de normes, procédures, outils et méthodes.

- Géré quantitativement (*Quantitatively Managed*)

La réussite des projets est quantifiée. Les causes d'écart peuvent être analysées.

- Optimisé (*Optimised*)

La démarche d'optimisation est continue.

2 Les normes de sécurité ISO 2700x pour la gouvernance sécurité

L'ISO (International Organisation for Standardisation) et le CEI (Commission Electrotechnique Internationale) définissent la norme comme : « *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*. »

La norme est un document de référence sur un sujet donné. Il indique l'état de la science, de la technologie et des savoir-faire au moment de la rédaction. La figure suivante illustre la famille de l'ISO 2700X.

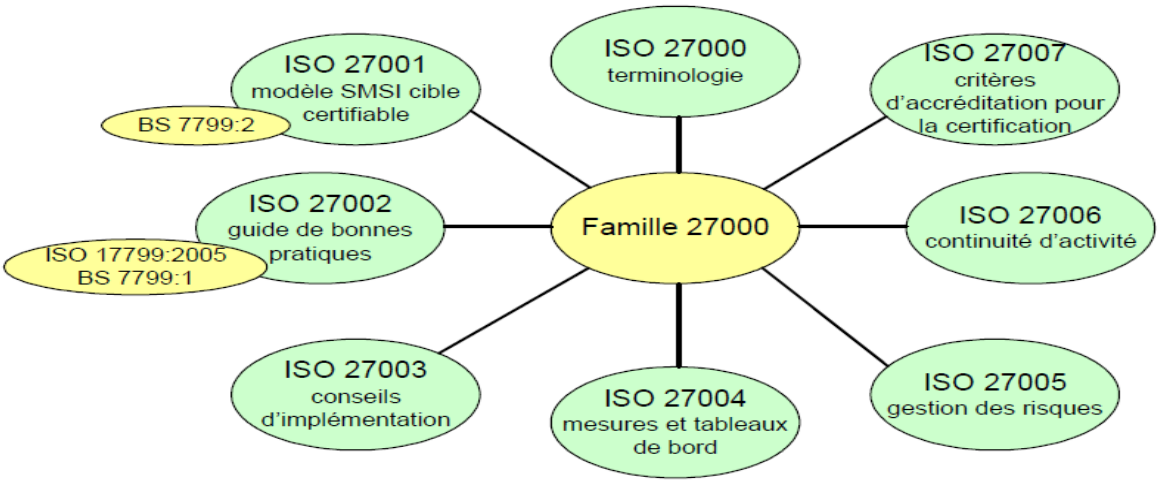


Figure 2.5 : La famille de normes ISO 27000

2.1 ISO 27001 Système de Gestion de la Sécurité de l'Information (ISMS)

La norme ISO 27001 instruit les personnes chargées de la sécurité dans les organisations comment bâtir, opérer, maintenir et améliorer un SMSI afin de préserver la sécurité de l'information traitée au sein de l'organisation. ISO 27001 remplace la deuxième partie du standard BS7799 **[23]** qui explique comment mettre en œuvre une démarche sécurité dans une organisation ; ISO 27001 reprend les bases de la BS 7799-2 avec en particulier son schéma de certification mature et éprouvé.

Ainsi, ISO 27001 complète ISO 27002 tout en ayant l'objectif d'aider les administrateurs des organisations à établir et maintenir un SMSI efficace en utilisant une démarche d'amélioration continue reconnue sous le nom de roue de Deming (PDCA : Plan-Do-Check-Act model) (Figure 15):

- PLAN (Etablir le SMSI) : il s'agit de déterminer le domaine du SMSI (i.e. ce qui doit être contrôlé par le SMSI) et exprimer les besoins en sécurité. Une politique de sécurité doit être définie exprimant les objectifs, les exigences de contrôle, les obligations contractuelles, l'organisation stratégique. Cette étape consiste aussi à réaliser l'analyse des risques et sélectionner les mesures à implémenter pour le traitement des risques.
- DO (Implémenter et opérer le SMSI) : Cette phase implémente le SMSI défini afin qu'il soit opérationnel. Elle consiste aussi à définir les plans de gestion des crises et de récupération d'activité.
- CHECK (Surveiller et réviser le SMSI) : La surveillance des opérations du SMSI

inclut la détection d'erreurs, l'audit des performances, l'identification de brèches de sécurité.

Cette phase assure aussi l'efficacité du SMSI et la prise en compte de risques résiduels (réévaluation de niveaux de risques acceptables et résiduels).

- ACT (Maintenir et améliorer le SMSI) : Le SMSI est amélioré par rapport aux résultats de la phase CHECK en prenant des actions correctives et préventives. Cette phase consiste aussi à valider les améliorations qui ont été apportées.

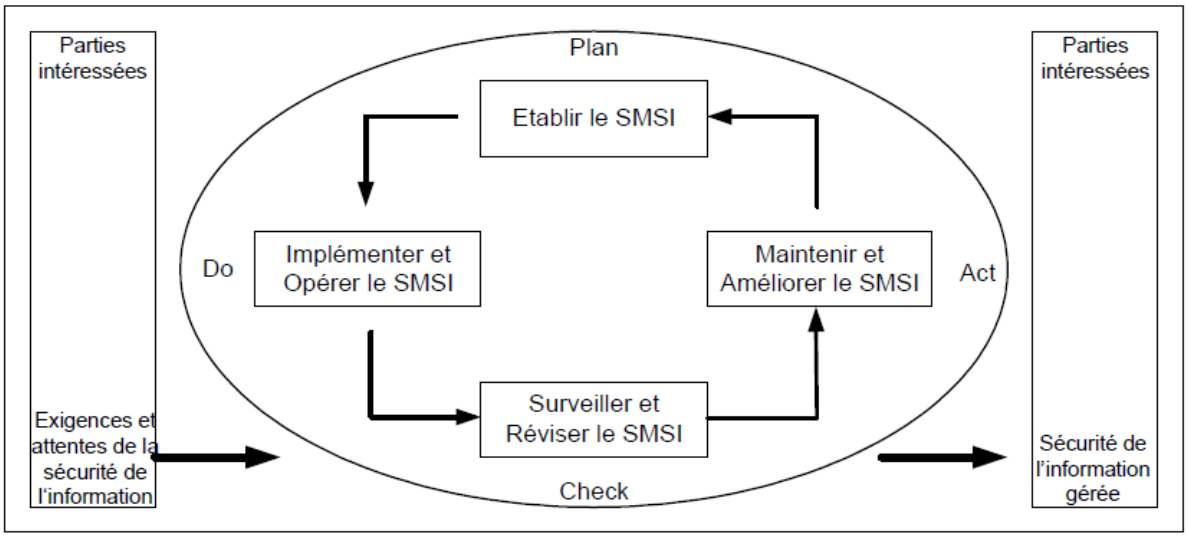


Figure 2.6 : Le modèle PDCA

La Figure 15 illustre le fait qu'un SMSI prend en entrée les exigences de la sécurité de l'information et les attentes des parties intéressées et, à travers les actions et les processus nécessaires, il fournit des résultats qui répondent à ces exigences et à ces attentes.

Une exigence pourrait être : les brèches de sécurité de l'information ne doivent pas causer de sérieux dommages financiers et/ou des embarras à l'organisation.

Une attente pourrait être : si un incident grave se produit (e.g. attaque du site web e-business de l'organisation), des personnes expérimentées ayant reçu des formations doivent être capables de réduire les impacts.

ISO 27001 est aligné avec ISO 9001 **[24]** et ISO 14001**[25]** afin de supporter une implémentation et une opération consistante et intégrée avec les normes de gestion connexes. Ainsi, un système de gestion bien conçu peut satisfaire les exigences de ces trois normes**[26]**.

ISO/IEC ISO 27002, dont le titre est : Code de bonnes pratiques pour la gestion de la sécurité de l'information, est publiée en juillet 2007 par l'ISO. Cette norme a pour objectif d'établir le label de confiance pour la sécurité globale de l'information de l'entreprise, tout comme ISO9000 représente un label pour le domaine de la qualité. Cette norme désire être un vecteur de communication à l'intention de partenaires dès lors que l'entité a besoin de :

2.2 27002 code de pratique pour la gestion des informations de sécurité

- répondre à des contraintes sur la sécurité de l'information,
- justifier d'un savoir-faire méthodologique dans la gestion de la sécurité de l'information.
- Se positionné par rapport à un référentiel international.

ISO 27002 fournit un recueil de bonnes pratiques de la sécurité de l'information applicables aux entreprises et organisations quel que soit leur taille ou leur secteur d'activité.

Elle propose un ensemble de mesures de sécurité (organisationnelles et techniques) sans toute fois imposer une solution technologique à adopter.

En 2000, ISO a adopté la première partie du standard BS7799 **[27]** publié par le British Standard Institute et l'a baptisée ISO 17799. En 2005, une version améliorée d'ISO 17799:2000 est apparue. ISO 17799:2005 contient onze sections spécifiant 39 objectifs de sécurité très généraux d'ordre théorique et 133 mesures (ou bonnes pratiques) à mettre en œuvre afin d'atteindre ces objectifs. Un objectif est défini comme étant le but à atteindre parla mise en œuvre des procédures de contrôle au sein d'une activité TI. Une mesure est définie comme étant les politiques, les procédures, les pratiques et les structures organisationnelles qui fournissent une assurance raisonnable que les objectifs métiers seront réalisés et que des évènements indésirables seront évités ou bien détectés et corrigés.

Ces mesures sont destinées à être utilisées par tous ceux qui sont responsables de la mise en place ou du maintien d'un SMSI.

ISO 27002 remplace la norme ISO 17799 depuis le 1er juillet 2007. Le contenu de la norme ISO 27002 est le même que celui de la norme ISO 17799:2005.

Ainsi, la norme ISO 27002 contient les onze sections (ou chapitres) déjà définis dans ISO 17799:2005. Les thèmes traités dans les différents chapitres sont :

- Politique de sécurité ;

- Organisation de la sécurité de l'information ;
- Gestion des biens (actifs) ;
- Sécurité liée aux ressources humaines ;
- Sécurité physique et environnementale ;
- Gestion de l'exploitation et des communications ;
- Contrôle d'accès ;
- Acquisition, développement et maintenance des systèmes d'information ;
- Gestion des incidents liés à la sécurité de l'information ;
- Gestion du plan de continuité de l'activité ;
- Conformité.

2.3 ISO/IEC 27003/2010 : Implémentation SMSI

ISO 27003 fournit une approche orientée processus pour la réussite de la mise en œuvre d'un SMSI conformément à l'ISO 27001 ; ISO/CEI 27003:2010 couvre le processus de spécification et de conception du SMSI, de la phase initiale à la production de plans d'exécution. La norme donne des recommandations sur la façon de convaincre la direction, ainsi que les différents concepts pour la conception et la planification d'un projet SMSI dont la réalisation sera un succès garanti. Destinée à être utilisée avec les normes ISO/CEI 27001:2005 et ISO/CEI 27002:2005, ISO/CEI 27003:2010 ne modifie, ni ne limite les exigences spécifiées dans ces deux normes.

Cette Norme internationale fournit des lignes directrices pratiques de mise en œuvre et apporte des informations complémentaires pour : l'établissement ; la mise en œuvre ; l'exploitation ; la surveillance ; le réexamen ; la mise à jour et l'amélioration d'un SMSI selon l'ISO/CEI 27001.

2.4 ISO/IEC 27004 Gestion de risque

Il est certain que le mesurage de la sécurité reste un sujet complexe qui reste mal appréhendé dans la plupart des SMSI. Sert à mesurer le niveau d'efficacité du SMSI mais également le niveau de sécurité de l'entreprise :

- c'est la démarche de gestion des risques et notamment le plan de traitement des risques qui peut lier le niveau de sécurité

- la mesure de l'efficacité d'un SMSI (de sa maturité ?) pourrait être dans l'absolu la dimension des incidents de sécurité (critiques et non critiques). Malheureusement sur quelle échelle temps?

2.5 ISO/IEC 27005 Gestion du risque en sécurité de l'information

La norme ISO/IEC 27005, intitulé « Gestion du risque en sécurité de l'information », est une évolution de la norme ISO 13335, définissant les techniques à mettre en œuvre dans le cadre d'une démarche de gestion des risques.

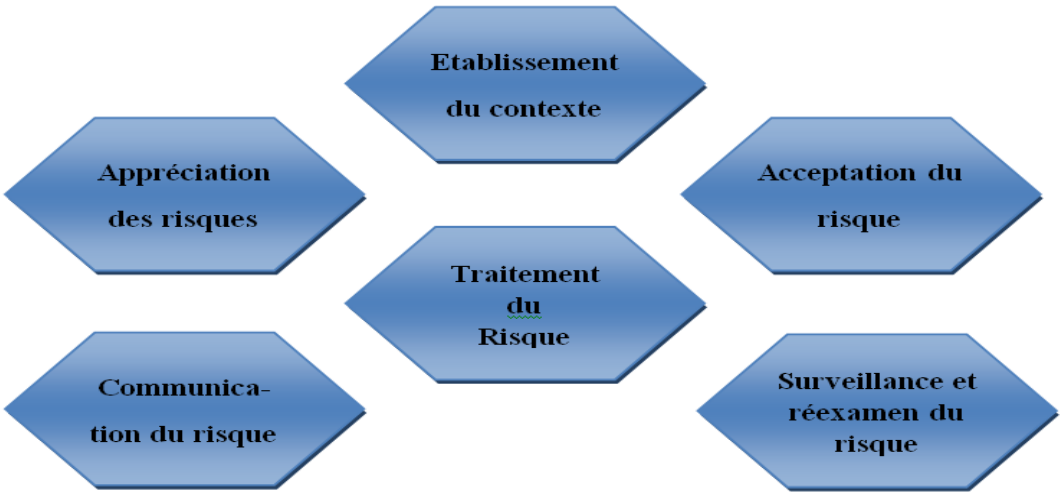


Figure 2.7 : Comment conduire le traitement des risques avec la norme ISO 27005

2.6 ISO/IEC 27006 Certification de SMSI

Exigences pour les organismes réalisant l'audit et la certification de SMSI; cette norme d'exigence (la seule de la série ISO 2700x avec ISO 27001) fournit des précisions pour les audits de certification ISO 27001:

- Classement des mesures de sécurité : organisationnelles / techniques
- Vérifications à faire ou pas pour les mesures de sécurité techniques
- Calcul du nombre de jours d'audit.

2.7 ISO 27007 Guide pour l'audit de (SMSI)

Cette norme s'appuiera sur la nouvelle version de la Norme ISO 19011 qui fixe les lignes directrices pour l'audit des systèmes de management de la qualité et de management environnemental **[28]**.

2.8 ISO 27008

Cette norme a pour principal objectif d'offrir des conseils sur la façon de vérifier ou confirmer la mesure dans laquelle les mesures de sécurité nécessaires sont mises en œuvre dans la pratique.

Elle fournit des indications sur l'analyse de la mise en œuvre et du fonctionnement des mesures de sécurité elles-mêmes (y compris la vérification de la conformité technique des mesures de sécurité) en conformité avec l'organisation de référentiels de sécurité de l'information établis **[29]**.

Synthèse

Les différents modèles que nous venons de présenter dans ce chapitre fournissent tous une forme d'évaluation de la confiance que ça soit dans les produits, les processus, les systèmes ou dans les pratiques implémentées. Pour synthétiser le tout, nous fournissons un tableau récapitulatif de l'ensemble des modèles cités dans ce chapitre (Tableau 2,1).

Résumé ou comparaison des ISO **2700X**

	Approche	**Axée sur la sécurité de l'information**	**Utilité**
Critères Communs	Orientée *produit*	Non	Evaluer la maturité d'un produit final
EBIOS - MEHARI	Orientée *gestion de risques*	Oui	Analyser et traiter les risques informatiques
ISO 27001 et ISO 27002	Orientée *meilleures pratiques* et *contrôles*	Oui	Définition/implémentation/ amélioration d'un SMSI (gestion de la sécurité)
ITIL	Orientée *processus*	Non	Gestion des services TI
COBIT	Orientée *processus*	Non	Gouvernance des services TI
CMMI	Orientée *processus*	Non	Evaluation des processus Informatiques

Tableau 2.1 : Comparaison des approches de gestion de la sécurité de l'information

Conclusion

Avec ces différents modèles qu'on a présenté, on peut constater le manque d'homogénéité et d'absence d'un modèle unifié offrant un cadre unique pour l'évaluation de la confiance considérée comme contrainte de base dans la construction d'une stratégie de sécurité. Cette pluralité de modèles rend cette construction un peu délicate et soumise à différents points de vue. Le chapitre suivent illustreras la norme 27002.

Chapitre 03 :La Normes ISO 27002

Introduction

Nous détaillons dans ce chapitre la norme 27002 qui répond à nos besoins et qui se figure dans la rubrique Plan de la roue de demming, d'où on présente sa définition son historique puis on passe à détailler l'ensemble de ses chapitres qui seront utilisés dans les prochaines parties, après on démontre son évolution et on termine par lister ses avantages et ses anomalies.

1 Définition

ISO/IEC 27002: **Code de bonne pratique pour la gestion des informations de sécurité :**La norme ISO/CEI 27002 est une norme internationale qui traite la sécurité de l'information, publiée en 2005 par l'ISO, dont le titre en français est *Code de bonnes pratiques pour la gestion de la sécurité de l'information.* Elle fait partie de la suite ISO/CEI 27000.

L'ISO/CEI 27002 est un ensemble de 133 mesures dites « best practices » (bonnes pratiques en français), destinées à être utilisées par tous ceux qui sont responsables de la mise en place ou du maintien d'un Système de Management de la Sécurité de l'Information (SMSI). La sécurité de l'information est définie au sein de la norme comme la « préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ».

Cette norme n'a pas de caractère obligatoire pour les entreprises, son respect peut toutefois être mentionné dans un contrat : un prestataire de services pourrait ainsi s'engager à respecter les pratiques normalisées dans ses relations avec un client **[28]**.

2 Historique

- En 1995, le standard britannique "BS 7799" qui fut créé par le "British Standard Institue" (BSI) définit des mesures de sécurité détaillées.
- En 1998, le BSI scinde le premier document en deux tomes : le BS 7799-1 correspondant aux codes des bonnes pratiques, et le BS 7799-2 correspondant aux spécifications d'un système de gestion de la sécurité de l'information (SMSI).
- En 2000, l'Organisation Internationale de normalisation (ISO) édite la norme ISO/CEI 17799:2000 correspondant aux codes des bonnes pratiques issues de la BS 7799.
- En 2005, deux normes sont éditées :

- ISO/CEI 17799:2005 qui remanie les domaines et objectifs
- ISO/CEI 27001:2005 qui introduit la notion de SMSI et offre la possibilité de certification.

En 2007, la norme ISO/CEI 17799:2005 étant obsolète, a été remplacée par la norme 27002 qui en reprend l'essentiel **[30]**.

3 Objectifs

ISO/CEI 27002 est plus un code de pratique, qu'une véritable norme ou qu'une spécification formelle telle que l'ISO/CEI 27001. Elle présente une série de contrôles (39 objectifs de contrôle) qui suggèrent de tenir compte des risques de sécurité des informations relatives à la confidentialité, l'intégrité et les aspects de disponibilité. Les entreprises qui adoptent l'ISO/CEI 27002 doivent évaluer leurs propres risques de sécurité de l'information et appliquer les contrôles appropriés, en utilisant la norme pour orienter l'entreprise.

La norme ISO 27002 n'est pas une norme au sens habituel du terme. En effet, ce n'est pas une norme de nature technique, technologique ou orientée produit, ou une méthodologie d'évaluation d'équipement telle que les critères communs CC/ISO 15408. Elle n'a pas de caractère d'obligation, elle n'amène pas de certification, ce domaine étant couvert par la norme ISO/CEI 27001 **[29]**.

4 Sommaire de l'ISO / CEI 27002 (Plan)

La carte mentale résume les principales sections de la norme sur un côté. Les chapitres sont décrits ci-dessous:

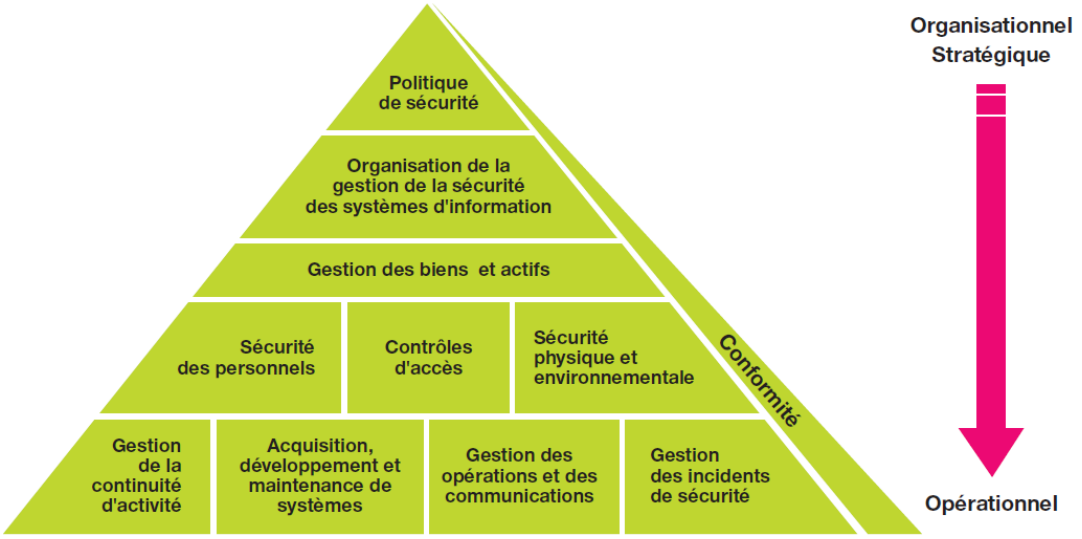


Figure 3.1 : les 11 chapitres de la norme ISO 27002

4.1 Chapitre N° 1 : Champ d'application

La norme donne des recommandations pour la gestion de la sécurité des informations pour ceux qui sont chargés de concevoir, mettre en œuvre ou le maintien de la sécurité.

4.2 Chapitre N° 2 : Termes et définitions

Sécurité de l'information est explicitement définie comme la «préservation de la confidentialité, l'intégrité et la disponibilité de l'information». Ceux-ci et d'autres termes connexes sont définies plus loin. Le moment venu, lorsque l'ISO / CEI 27002 est révisée, cette section sera vraisemblablement définitions de référence dans l'ISO / CEI 27000.

4.3 Chapitre N° 3 : Structure de la présente norme

Cette page explique simplement que les tripes de la norme contiennent des objectifs de contrôle, a suggéré la mise en œuvre des contrôles et d'orientation.

4.4 Chapitre N° 4 : Évaluation des risques et de traitement

ISO / CEI 27002 couvre le sujet de la gestion des risques en à peine une page et demie, la couverture malheureusement insuffisant pour un tel élément complexe et du centre de sécurité de l'information. Lorsque l'ISO / CEI 27002 est révisée, elle sera probablement ISO de référence/ IEC 27005 ici bien qu'il ait été suggéré que la section de gestion des risques pourraient être abandonnées entièrement à partir 27002 et déplacé à l'27001. En accord avec le style de 27002, 27005 donne des directives générales sur la sélection

et l'utilisation de méthodes appropriées pour analyser les risques pour la sécurité des informations il ne prescrit pas une méthode spécifique, puisque «appropriée» dépend du contexte.

4.5 Chapitre N° 5 : Politique de sécurité de l'information

La direction devrait définir une politique visant à clarifier leur direction, et le soutien des renseignements sur la sécurité, ce qui signifie une brève information de haut niveau énoncé de politique de sécurité fixant les directives de sécurité des informations essentielles et les mandats pour toute l'organisation. Ceci est normalement pris en charge par un vaste Suite des politiques de l'information plus détaillée des sociétés de sécurité, habituellement sous la forme d'une politique d'information du Manuel de la sécurité. Le manuel de politique à son tour, est soutenu par un ensemble de normes de sécurité de l'information, des procédures et lignes directrices . Bien que les normes sont quelque peu ambigus sur ce point, la politique de sécurité de l'information a noté dans l'ISO / CEI 27002 est généralement considéré comme séparé et différent de la politique SMSI requises par l'ISO / CEI 27001. SMSI La politique est perçue par certains comme une stratégie ou gouvernance papier portant sur l'appui de la direction pour le SGSI dans son ensemble - en fait, elle mai être le plus court à une déclaration du directeur général.

4.6 Chapitre N° 6 : Organisation de la sécurité de l'information

Une structure de sécurité d'information adapté et de gouvernance devraient être conçues et mises en œuvre.

- **Organisation interne**

Les rôles et les responsabilités doivent être définis pour la fonction de sécurité de l’information.

Les accords de confidentialité doit refléter les besoins de l'organisation. Des contacts devraient être établis avec les autorités compétentes (Application de la loi) et des groupes d'intérêts spéciaux. Sécurité de l'information devrait être revue de manière indépendante.

- **Parties externes**

Sécurité de l'information ne doit pas être compromise par l'introduction de produits ou services de tiers, les risques doivent être évalués et atténués, lorsqu'ils traitent avec les clients et dans les accords de tiers.

4.7 Chapitre N° 7 : Gestion des actifs

L'organisation devrait être en mesure de comprendre ce que les ressources d'information qu'il détient, et de gérer leur sécurité de manière appropriée.

- **Responsabilité pour les actifs**

Toutes les informations et les actifs doivent être comptabilisés et avoir un propriétaire désigné. Un inventaire des actifs informationnels (matériel informatique, logiciels, données, documentation du système, supports de stockage, en soutenant des actifs tels que les climatiseurs individuels ordinateur et onduleurs et des services TIC) devraient être maintenu.

L'inventaire devrait enregistrer la propriété et la localisation des actifs, et les propriétaires devraient déterminer les utilisations acceptables.

- **Classification de l'information**

L'information devrait être classée en fonction de son besoin de protection de la sécurité et étiquetés en conséquence. Tout cela est clairement plus pertinentes aux militaires et aux organisations gouvernementales de manipulation « des informations marquées» (Top Secret, …etc.).

Le concept d'identification des actifs importants, de classement et regroupement eux, et l'application de contrôles qui sont jugés appropriés pour les actifs de cette nature, est largement applicable.

4.8 Chapitre N° 8 : Sécurité liée aux ressources humaines

Il donne les recommandations destines à réduire le risque d'erreur ou de fraude en favorisant la formation et la sensibilisation des utilisateurs sur les risqué et les menaces pesant sur les informations.

- **Avant à l'emploi**

Responsabilités de sécurité devraient être prises en considération lors du recrutement des employés permanents, entrepreneurs et agents temporaires (A travers des descriptions d'emploi adéquates, le dépistage pré-emploi) et inclus dans les contrats (Termes et conditions d'emploi et d'autres accords signés sur les rôles et les responsabilités de sécurité).

- **En cours d'emploi**

Responsabilités de la direction concernant la sécurité des informations doivent être définies. Employés et (s'il ya lieu) un tiers des utilisateurs de TI doivent être sensibilisés,

éduqués et formés dans les procédures de sécurité. Un processus disciplinaire formel est nécessaire pour traiter les infractions de sécurité.

- **Résiliation ou changement d'emploi**

Aspects de sécurité de la sortie d'une personne de l'organisation (Le retour de biens sociaux et la suppression des droits d'accès) ou de changement de responsabilités devraient être gérés.

4.9 Chapitre N° 9 : Sécurités physiques et environnementales

Précieux matériel informatique doivent être physiquement protégés contre les dommages intentionnels ou accidentels ou la perte, la surchauffe, la perte de conduites d'alimentation,

- **Zones sécurisées**

Cette section décrit la nécessité pour les couches concentriques de contrôles physiques pour protéger les installations sensibles IT des accès non autorisés.

- **Sécurité des installations**

Critiques matériel informatique, le câblage et ainsi de suite doivent être protégés contre les dommages physiques, incendie, inondation, vol,… etc., à la fois sur et hors site, l'alimentation électrique et le câblage doivent être assurés. IT équipement doit être entretenu comme il convient et éliminés de façon sûre.

4.10 Chapitre N° 10 : Exploitation et gestion des communications

Cette longue section détaillée de la norme décrit les contrôles de sécurité des systèmes et la gestion du réseau.

- **Les procédures opérationnelles et les responsabilités**

Les responsabilités opérationnelles et les procédures doivent être documentées. Les changements des installations des systèmes devraient être contrôlés. Les droits devraientêtre répartis entre différentes personnes, le cas échéant (Accès au développement et les systèmes d'exploitation doivent être distincts).

- **Tiers fournisseurs de services de gestion de livraison**

Les exigences de sécurité devraient être prises en compte dans la prestation de services tiers (TI ou l'externalisation de la gestion des installations), de clauses contractuelles

à la surveillance continue et la gestion du changement. Avez-vous clauses de sécurité appropriées dans le contrat avec votre FAI?

- **Planification de systèmes et d'acceptation**

IT couvre la planification des capacités et des processus d'acceptation de production.

- **Protection contre les codes malicieux et mobiles**

Décrit la nécessité pour les contrôles anti-logiciels malveillants, y compris la sensibilisation des utilisateurs. Les contrôles de sécurité pour le code mobile sont également décrits.

- **Sauvegardes**

Couvertures de routine des sauvegardes de données et la restauration des répétitions.

- **Gestion de la sécurité des réseaux**

Les grandes lignes de gestion de réseau sécurisé, suivi de la sécurité réseau et d'autres contrôles. Couvre également la sécurité des réseaux de services commerciaux tels que les réseaux privés et la gestion des pare-feu, …etc.

- **Gestion des supports**

Les modalités de fonctionnement devraient être définies pour protéger des documents et des supports informatiques contenant des données, informations, et système. Élimination des supports de sauvegarde, les documents, enregistrements vocaux et autres données d'essai,…etc.

Des procédures devraient être définies pour la manipulation en toute sécurité, le transport et le stockage des supports de sauvegarde et de la documentation du système.

- **L'échange d'informations**

Les échanges d'information entre les organisations doivent être contrôlées, par exemple, même si les politiques et procédures, et des accords juridiques. Les échanges d'information doivent également se conformer à la législation applicable. Les procédures de sécurité et les normes devraient être en place pour protéger l'information et des supports physiques en transit, y compris la messagerie électronique (e-mail, EDI) et des systèmes d'information commerciale.

- **Services de commerce électronique**

Les implications de sécurité du commerce électronique (systèmes de transaction en ligne) doivent être évaluées et des contrôles appropriés mis en œuvre. L'intégrité et la disponibilité des informations publiées en ligne (Les sites Internet) devraient également être protégées.

- **Surveillance**

Couvre des événements de sécurité ; audit ; d'enregistrement d'erreurs et de système d'alarme ; surveillance et d'alerte pour détecter l'utilisation non autorisée, couvre également la nécessité d'obtenir des billes et de synchroniser les horloges système.

4.11 Chapitre N° 11 : Contrôle d'accès

L'accès logique aux systèmes informatiques, les réseaux et les données doivent être convenablement contrôlée pour éviter toute utilisation non autorisée.

- **Exigences des entreprises pour le contrôle d'accès**

Exigences de l'organisation pour contrôler l'accès à l'information des actifs devraient être clairement documentés dans une politique de contrôle d'accès, y compris pour exemple: emploi profils d'accès connexes.

- **Utilisateurs de gestion des accès**

L'attribution de droits d'accès aux utilisateurs devraient être officiellement contrôlé par l'enregistrement des utilisateurs et des procédures administratives (de l'inscription initiale de l'utilisateur par le biais de la suppression des droits d'accès lorsqu'il n'est plus nécessaire), y compris des restrictions spéciales sur l'attribution des privilèges et la gestion des mots de passe, et un accès régulier les droits de commentaires.

- **Responsabilités des utilisateurs**

Les utilisateurs doivent être conscients de leurs responsabilités en vers l'accès effectif de maintenir des contrôles, par exemple, systèmes et information doivent être assurés lorsqu'ils sont laissés sans surveillance.

- **Contrôle d'accès au réseau**

L'accès aux services en réseau devrait être contrôlé, tant au sein de l'organisation et entre organisations. La politique devrait être définie et utilisateurs distants (et éventuellement du matériel) doivent être dûment authentifiés. Ports éloignés de diagnostic doivent être bien

contrôlés. Les services d'information, les utilisateurs et les systèmes devraient être séparés dans des domaines de réseau distinct logique. Connexions réseau et de routine doit être contrôlée si nécessaire.

- **Le système d'exploitation contrôle d'accès**

L'exploitation d'installations de contrôle d'accès au système et les services publics (tels que l'authentification des utilisateurs avec des identifiants et mots de passe d'utilisateur unique gérée, pour enregistrer l'utilisation de privilèges et d'alarmes de sécurité du système) doit être utilisée. L'accès aux services publics puissant système doit être contrôlée et délais d'inactivité devrait être appliqué.

- **Application et contrôle d'accès d'information**

L'accès à et dans les systèmes d'application devraient être contrôlés en conformité avec une politique définie contrôle d'accès. Notamment des applications sensibles mai exigent dédié (isolé) des plates-formes, et / ou contrôles supplémentaires si elles sont exécutées sur des plateformes communes.

- **L'informatique mobile et le télétravail**

Il devrait y avoir de politique officielle concernant l'utilisation sécurisée des PC portables, PDA, téléphones cellulaires, ainsi que le télétravail sécurisé («travail à domicile», et d'autres formes de travail mobile ou à distance).

4.12 Chapitre N° 12 : Acquisition, développement et maintenance des systèmes d'informations

La sécurité des informations doit être pris en compte dans le cycle de développement des systèmes (CCES) les procédés de spécification, de construction / acquisition, les essais, la mise en œuvre et maintenir des systèmes informatiques.

- **Exigences de sécurité des systèmes d'information**

Manuelles et automatiques de contrôle des exigences de sécurité devraient être analysées et pleinement identifiés pendant l'étape exigences de développement des systèmes ou des processus d'acquisition, et incorporée dans les cas d'affaires. Acheté en logiciels devraient être testés officiellement pour la sécurité, et de tout risque questions-évaluées.

- **Traitements corrects dans les systèmes d'application**

La saisie des données, le traitement et les contrôles de validation de sortie et d'authentification de message devrait être fournie pour atténuer les risques pour l'intégrité sont associés.

- **Contrôles cryptographiques**

Une politique de cryptographie doit être définie, concernant les rôles et les responsabilités, les signatures numériques, la non-répudiation, la gestion des clés et certificats numériques,….etc.

- **Sécurité des fichiers système**

L'accès aux fichiers du système (programmes exécutables et code source) et données d'essais devrait être contrôlée.

- **Sécurité dans le développement et soutenir les processus**

Gestionnaires du système de demande devraient être chargés de contrôler l'accès aux développements des projets et des environnements de soutien. Formelle des processus de changement de contrôle doit être appliquée, y compris des examens techniques. Par exemple via des canaux cachés et chevaux de Troie, si ceux-ci sont une préoccupation. Un certain nombre de surveillance et des contrôles de surveillance sont présentées pour le développement externalisé.

4.12.1 Techniques de gestion des vulnérabilités

Vulnérabilités techniques dans les systèmes et les applications doivent être contrôlés par la surveillance de l'annonce des failles de sécurité pertinentes, et le risque-évaluer et appliquer les correctifs de sécurité applicables rapidement.

4.13 Chapitre N° 13 : Gestion des incidents

Sécurité de l'information événements, des incidents et des faiblesses (y compris les quasi-accidents) doit être signalé sans délai et correctement gérées.

- **Reportions dans les événements de sécurité de l'information et des faiblesses**

Une déclaration d'incident ou de la procédure d'alarme est demandée, plus la réponse associée et les procédures d'escalade. IL devrait y avoir un point de contact central, et tous les employés, les entrepreneurs, devraient être informés de leurs rapports d'incidentes responsabilités.

4.13.1 Gestion des incidents de sécurité de l'information et des améliorations

Les responsabilités et les procédures sont requises pour gérer les incidents de façon cohérente et efficace, à mettre en œuvre l'amélioration.

4.14 Chapitre N° 14 : Gestion de la continuité d'activité

Cette section décrit la relation entre les TI de planification de reprise après sinistre, la gestion de continuité des opérations et planification d'urgence, allant de l'analyse et la documentation grâce à l'exercice régulier / test des plans. Ces contrôles visent à minimiser l'impact des incidents de sécurité qui se produisent en dépit des contrôles préventifs noté par ailleurs dans la norme.

4.15 Chapitre N° 15 : Conformité

Il traite :

- le respect des lois et des réglementations ;
- la conformité des procédures en place au regard de la politique de sécurité ;
- l'efficacité des dispositifs de traçabilité et de suivi des procédures, notamment les journaux d'activités, les audits et les enregistrements de transactions.

- **Conformité aux exigences légales**

L'organisation doit se conformer à la législation applicable, comme le copyright, protection des données, protection des données financières et autres actes d'état civil, les restrictions à la cryptographie,...etc.

- **Conformité avec les politiques et normes de sécurité et de conformité technique**

Les gestionnaires et les propriétaires de système doit assurer la conformité avec les politiques et normes de sécurité, par exemple grâce à des examens réguliers plate-forme de sécurité, tests de pénétration, etc.

- **Systèmes d'information des considérations d'audit**

Les audits devraient être soigneusement planifiés pour minimiser les perturbations pour les systèmes opérationnels.

De puissants outils d'audit / installations doivent également être protégés contre toute utilisation non autorisée **[28].**

5 Evolution de la norme entre les versions ISO 27002:2005 et ISO 27002:2013 :

Cette évolution largement attendue permet de supprimer des mesures de sécurité obsolètes de clarifier des mesures précédemment incompréhensibles, ainsi qu'une restructuration bénéfique de certains chapitres.

On peut citer le découpage de l'ancien chapitre 10 : exploitation et gestion des communications, qui faisait à lui seul presque un quart du document en deux chapitres distincts : Sécurité liée à l'exploitation et Sécurité des communications

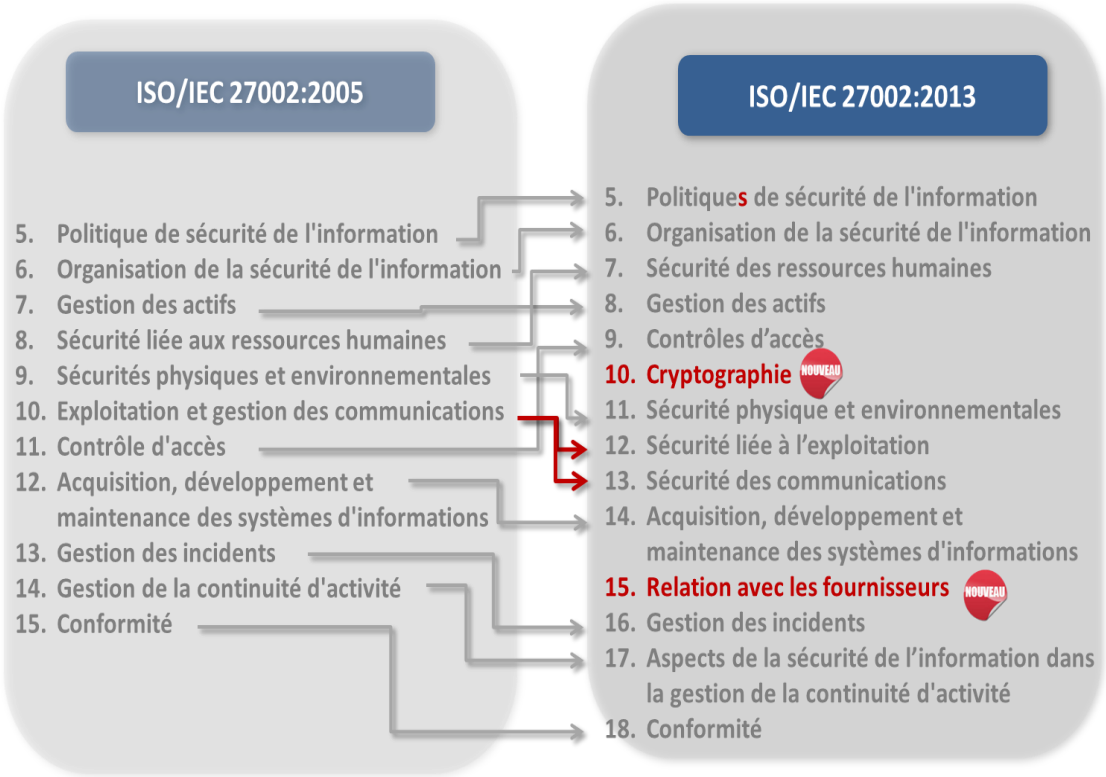


Figure 3.2 : Evolution de la norme entre les versions 2005 et 2013

6 L'intérêt de la norme ISO 27002:2013 ... et ses limites

Le premier intérêt d'utiliser ISO 27002 est évidemment sa diffusion et sa reconnaissance internationale. Un consensus est acquis sur le domaine couvert par la sécurité de l'information (versus le seul périmètre de la sécurité informatique) et sa structuration par domaine.

Cela permet ainsi une simplification dans l'utilisation de méthodes de sécurité , parler le même langage de la communication entre sociétés ou entités d'une même entreprise, ensuite, l'ensemble des mesures de sécurité qui y sont définies peuvent être considérées comme les bonnes pratiques actuelles.

Mais il faut également considérer les limites d'ISO 27002. La plus sérieuse est qu'elle ne permet pas de définir quelles est les mesures de sécurité à mettre en œuvre en fonction du contexte de l'entreprise.

Ainsi, il est aberrant d'imaginer qu'il faut mettre en œuvre l'ensemble des mesures de sécurité décrites dans la norme (pour des questions de coût et de besoins réels). Il faut démarrer la démarche par une analyse des enjeux et des risques.

La seconde limite est liée au cycle de normes ISO, en effet une évolution de norme prend environ 5 ans. Dans le domaine des technologies de l'information, les menaces potentielles et les mesures de sécurité liées évoluent plus rapidement que cela.

7 Les avantages

1. Organisation: image positive auprès des actionnaires lorsque l'entreprise tend à maîtriser ses risques pour maximiser ses profits
2. Conformité: la norme insiste sur la nécessité d'identifier toutes les lois et réglementations s'appliquant à l'entreprise et la mise en œuvre de processus adaptés pour identifier et suivre les obligations permet de prouver au moins la volonté de conformité, ce qui tend à diminuer les amendes en cas de non-conformité
3. Gestion des risques: la norme insiste dans ses chapitres d'introduction sur la nécessité de réaliser une analyse de risques périodiquement et définit dans les domaines « politique de sécurité » et « organisation de la sécurité » les pratiques à mettre en œuvre pour gérer les risques mis en lumière par l'analyse de risque. Ceci permet une meilleure connaissance des risques et donc une meilleure allocation des ressources permettant d'améliorer la fiabilité du système.
4. Finances: associant une meilleure maîtrise des risques, une meilleure gestion des incidents et une meilleure allocation des ressources, la mise en place d'un SMSSI s'appuyant sur les normes ISO 27001 et 27002 permet une meilleure maîtrise des coûts de la sécurité des systèmes d'information.
5. Crédibilité et confiance: la mise en place d'une politique de sécurité et des moyens associés donne une image rassurante pour les partenaires et les clients, notamment sur la protection des données personnelles (sujet très médiatique, avec le syndrome du« Big Brother »).
6. Ressources humaines: s'appuyer sur une norme permet de mieux faire passer les messages de sensibilisation, notamment auprès des populations techniques **[30].**

Conclusion

On a présenté la norme ISO 27002 Code de bonne pratique pour la gestion des informations de sécurité, On utilisera cette norme, dans le prochain chapitre pour l'opération d'audit sur la sécurité des systèmes d'information effectuée au sein de l'université 8 mai 1945 Guelma.

Chapitre 04 : Audit du SSI de l'université 8 Mai 1945

Introduction

Dans ce chapitre nous présentons l'opération d'audit sur la sécurité des systèmes d'information effectuée au sein de l'université 8 mai 1945 Guelma, pour cela nous commençons d'abord par présenter le contexte et l'objectif de cette audit, puis une synthèse sur ce projet.

1. Présentation générale l'université

L'université 8 Mai 1945 est un établissement public à caractère scientifique, culturel et professionnel doté de la personnalité morale et de l'autonomie financière. Elle a connu 04 importantes étapes de son existence, d'abord des instituts nationaux de l'enseignement supérieur de Guelma ont été créés en 1986, devenus ensuite centre universitaire par le décret 92-299 du 07/07/1992, puis université par le décret exécutif N° 01-273 du 30 septembre 2001 qui l'organise en 03 facultés, réorganisée en sept (07) facultés par le décret exécutif N°10-16 du 21 janvier 2010.

Figure 4.1: logo de l'université du 8 mai 1945 -Guelma-

A présent, elle assure un enseignement pluridisciplinaire en graduation et post-graduation en trente filières d'enseignement sur les trois niveaux licence, master et doctorat. Actuellement les structures de l'université de Guelma sont implantées sur quatre (4) sites

- **Campus Souidani Boudjemââ :** qui abrite deux facultés à savoir **:**

1. La Faculté des Sciences Economiques, commerciales et des sciences de gestion : elle comprend trois filières:

- Département des sciences de gestion
- Département des Sciences commerciales
- Département des sciences économiques

2. La Faculté des Sciences Humaines et Sociales : elle se compose de trois départements à savoir:
   - ❖ Département des Sciences Humaines
   - ❖ Département des Sciences Sociales
   - ❖ Département d'histoire et archéologie

- **L'ancien campus :** abrite deux facultés à savoir **:**

1. La faculté de Technologie : elle comprend cinq départements Suivants: (Génie procédé, génie mécanique, Génie civil, électrotechnique et automatique et électronique télécommunication).

2. La faculté des mathématiques et de l'informatique et des sciences de la matière rassemble trois branches à savoir : Sciences de la matière, Mathématiques et Informatique.

- **Le nouveau Campus :** abrite le rectorat de l'université **:**

1. La Faculté des Sciences de la Nature et de la Vie et Sciences de la Terre et de L'univers se compose de trois départements :
   - ➢ Département de Sciences de la Nature et de la Vie
   - ➢ Département de biologie
   - ➢ Département d'écologie et du génie de l'environnement

2. Faculté des lettres et des langues

- **Le campus d'Héliopolis :**

1. La Faculté de Droit et Sciences Politiques se compose de :
   - ➢ Département des sciences juridiques et administratives
   - ➢ Département des sciences politique.

En matière d'équipement informatique, l'université dispose de :

- Environ 900 postes de travail
- Environ 15 serveurs en exploitation
- Un centre de calcul intensif.
- Un réseau local qui couvre la totalité de l'université, c.à.d. tous les campus sont interconnectés.
- Gestion du parc informatique : décentralisée.
- Les blocs sont géographiquement distants.

1.1 I.1 L'organigramme de l'université

<table>
<tr><td colspan="5">Le recteur</td></tr>
<tr><td colspan="2">- Conseil d'administration de l'université
- Conseil scientifique de l'université
- Comité local d'éthique et de déontologie
- Bibliothèque centrale</td><td colspan="3">- Le Vice rectorat de la formation supérieure de troisième cycle, l'habilitation universitaire, la recherche scientifique et la formation supérieure de post-graduation
- Vice rectorat de la formation supérieure du premier et deuxième cycles, la formation continue et les diplômes, et la formation supérieure de graduation
- Vice rectorat des relations extérieures, la coopération, l'animation, la communication et les manifestations scientifiques
- Vice-Rectorat du développement, de la prospective et de L'orientation</td></tr>
<tr><td colspan="2">- Sous-direction des personnels
- Sous-direction des finances et comptabilité
- Sous-direction des moyens généraux
- Sous-direction des activités scientifiques culturelles et sportives</td><td colspan="3">Facultés</td></tr>
<tr><td colspan="2" rowspan="3">Centre d'enseignement intensif des langues
Centre commun des réseaux et systèmes d'information et de la communication
Direction de la publication universitaire
Unités de médecine préventive</td><td>Facultés des sciences et de la technologie</td><td>Faculté de droit et des sciences</td><td>Faculté des lettres et des langues</td><td>Faculté des sciences humaines et sociales</td></tr>
<tr><td colspan="4">Faculté de mathématiques et de l'informatique et des sciences de la matière</td></tr>
<tr><td colspan="4">Faculté des sciences de la nature et de la vie et sciences de la terre et de l'univers</td></tr>
<tr><td colspan="4">Faculté des sciences économiques, commerciales et des sciences de gestion</td></tr>
</table>

1.2 Centre commun de réseaux, de systèmes d'information et de la communication et de télé-enseignement (CCRSIC)

1.2.1 Présentation du centre

Le centre commun de réseaux, de systèmes d'information et de la communication et de télé-enseignement qui se trouve à l'ancien campus a été créé le 6 Juin 2007, sa mission principale est l'utilisation des technologies de l'information et de la communication (TIC) dans l'enseignement supérieur, chargé de :

- l'exploitation, l'administration et la gestion des infrastructures des réseaux ;
- l'exploitation et le développement des applications informatiques de gestion de la pédagogie ;

- le suivi et l'exécution des projets de télé-enseignement et d'enseignement à distance ;
- assurer l'appui technique à la conception et la production de cours en ligne ;
- la formation et l'encadrement des intervenants dans l'enseignement à distance.

Il comporte les sections suivantes :

- section des systèmes ;
- section des réseaux ;
- section de télé-enseignement et enseignement à distance.

Ce centre est organisé comme suit :

- Salle de cours ;
- Salle de visioconférences ;
- Cellule de production ;
- Site web de l'université .

Salle de cours

Offrir aux apprenants des outils technologiques (ordinateurs, logiciels, Internet) pour poursuivre des formations accessibles via Internet.

Salle de visioconférences

- Réception par Internet de conférences animées par des intervenants externes (En Algérie ou depuis l'étranger) .
- Projection de conférences avec des intervenants présents sur place pouvant utiliser le PC, la Caméra document, ...etc.

Cellule de production

- Conception et production de contenus par des équipes pluridisciplinaires regroupant des enseignants, des pédagogues et des ingénieurs informaticiens.
- Gestion de projets de formation basée sur les TIC (Technologies de l'Information et de la Communication).

2. Le périmètre de la PSSI à l'université

La politique de sécurité des systèmes d'information de l'université s'applique dans un cadre globale à l'ensemble du système d'information de l'université, elle comprend l'ensemble des moyens humains, techniques et organisationnels. Elle s'applique à :

- ✓ l'ensemble des personnels autorisés à accéder, utiliser ou traiter, au niveau fonctionnel ou technique, des informations ou des biens des Systèmes d'Information;
- ✓ l'ensemble des tiers (fournisseur, prestataire de service, personnes invités dans le cadre des séminaires,…), dès lors qu'ils utilisent les Systèmes d'Information ou que

leurs propres Systèmes d'Information sont reliés au réseau informatique du l'université;

- ✓ l'ensemble du patrimoine informationnel quel qu'en soit le support ou la nature ;
- ✓ tous les composants matériel et logiciel des systèmes d'information, afin de garantir les points suivants :

1. Une Confidentialité : La confidentialité est la propriété qu'une information n'est ni disponible ni divulguée aux personnes, entités ou processus non autorisés.
2. Une Disponibilité : Propriété d'accessibilité au moment voulu des données et des fonctions par les utilisateurs autorisés.
3. Une Intégrité : L'intégrité est la prévention d'une modification non autorisée de l'information.

3. Contexte de PSSI

3.1 Engagement de la direction

L'université ne possède pas une politique de sécurité formalisée. Notre projet a pour objectif l'élaboration d'un cadre globale de sécurité

L'administration de l'université est consciente de l'importance de développer une politique de sécurité en par le lançant ce projet. L'engagement de l'administration s'est traduit par un mandat d'élaboration d'une politique de sécurité. Le mandat a été discuté avec le CCRSIC. Les thèmes abordés lors de la définition du mandat ont été:

- ➢ Les objectifs poursuivis par la direction en matière de sécurité de l'information. Par exemple : se conformer aux lois, assurer la sécurité des usagers, …etc;
- ➢ l'engagement de la haute direction à participer activement à l'exercice. Le support de la direction est particulièrement crucial lors des étapes de recensement des préoccupations, de validation et d'adoption;
- ➢ La disposition de personnel spécialisé au demain.

L'annexe A présente un fiche-mandat de projet.

3.2 Approche adopté

Pour bien déterminer le contexte de sécurité PSSI, nous avons adopté une approche qui consiste à mesurer le niveau de maturité en se basant sur un questionnaire issu de la Norme ISO 27002 (**voir annexe B**).

Ce questionnaire comporte 11 chapitres, chaque chapitre présente un thème de sécurité dans lequel sont exposés des objectifs de contrôles et des recommandations sur les mesures de sécurité à mettre en œuvre et les contrôles à implémenter.

3.3 Audit de SSI de l'université 8 mai 1945

3.3.1 Objectifs de l'audit

Dans le but de disposer d'un état des lieux, nous avons effectué une opération d'audit de la SSI sous la tutelle du CCRSIC de l'université, l'audit a pour objectif :

- D'identifier les points faibles de la SSI,
- Proposer des recommandations pour l'amélioration.

La mission d'audit a donné lieu à produire d'un rapport destiné à l'administration de l'université contenant:

- L'ensemble des travaux d'audit de la SSI, constats et recommandations.
- Les résultats de l'audit de la SSI.

4. Synthèse

4.1 Le projet d'élaboration d'une PSSI

Notre travail s'inscrit dans le cadre de l'engagement de la direction de l'université de Guelma à établir une politique de sécurité basée sur une opération d'audit, pour cela on a commencé cette opération depuis le mois de février 2015, dans l'absence de toute sorte de documentation sur la sécurité informatique d'une manière générale afin d'atteindre l'objectif cité auparavant.

4.2 Contexte et modalités de réalisation

L'équipe de travail a réalisé un audit auprès des informaticiens du centre d'informatique de l'université. Le but de l'audit est de permettre à des personnes concernées d'exprimer leurs avis sur le PSSI, leurs suggestions et éventuellement leur participation à son amélioration.

4.3 Modalités de réalisation et périmètre des travaux d'audit

4.3.1 Modalités de réalisation

Une équipe de réalisation de l'audit a été désignée par l'administration et s'est réuni plusieurs fois afin de préparer sa mission. Elle est composée de :

- M. NOUAR Fayçal, enseignant informaticien, responsable de la mission et chef du centre d'informatique de l'université

- Mlle. BOUKHALFA Fatima Zahra, étudiante en 2ème année, sciences de gestion, spécialité Technique de l'Information et de Communication dans l'entreprise (TIC), promotion 2015, faculté des sciences économiques, de gestion et des sciences commerciales (SEGC).
- Mme. HAFARESSAS Khadidja, étudiante en 2ème année, sciences de gestion, spécialité Technique de l'Information et de Communication dans l'entreprise (TIC), promotion 2015, faculté des sciences économiques, de gestion et des sciences commerciales (SEGC).
- M. CHELAGHMIA Abdel Malek, ingénieur informaticien à l'université de Guelma.
- Mme. SEDRAOUI Soumya ; ingénieur informaticienne à l'université de Guelma.

L'audit a été réalisé entre le 01/02/2015 jusqu'au 25/05/ 2015.

4.3.2 Périmètre des travaux d'audit

Les travaux d'audit ont pris en considération l'ensemble des points ayant liens avec le SI de l'université. L'enquête a été réalisée sous la tutelle de l'administration. Cependant, les limites suivantes s'appliquent aux travaux d'audit réalisés :

- Des entretiens ont été réalisés avec Responsable et le personnel du CCRSIC.
- Les travaux réalisés n'avaient pas pour objectifs d'effectuer des tests techniques approfondis.

4.3.3 Audit du SSI :

Le constat d'audit, ainsi que le niveau de criticité sont résumés ci-dessous. Les niveaux de criticité sont les suivants :

🔴 **Majeur** : Les points correspondants doivent être traités dans les plus brefs délais. Les Faiblesses sous-jacentes induisent un risque majeur pour l'université de ne pas atteindre ses Objectifs, aux processus sous-jacents de ne pas délivrer le service correspondant aux attentes.

🟡 **Moyen :** Il s'agit de faiblesses qui pèsent actuellement sur le SI et qui pourraient induire Des risques de non-conformité ou induire service dégradé fourni par le SI. Les points Correspondant pourraient être traités dans deuxième temps ou en priorité si la recommandation est simple à mettre en œuvre.

🟢 **Faible** : Il s'agit de points qui indiquent des non-conformités aux bonnes pratiques. Ces non-conformités ne génèrent pas de risques significatifs sur le SI et sur les objectifs perçus durant l'audit.

5. Présentation et interprétation des résultats

Lors de cette intervention et suivant les réponses aux questionnaires, nous avons pu déceler les constations suivantes :

5.1 Politique de sécurité de l'information (domaine N°5):

Résultat

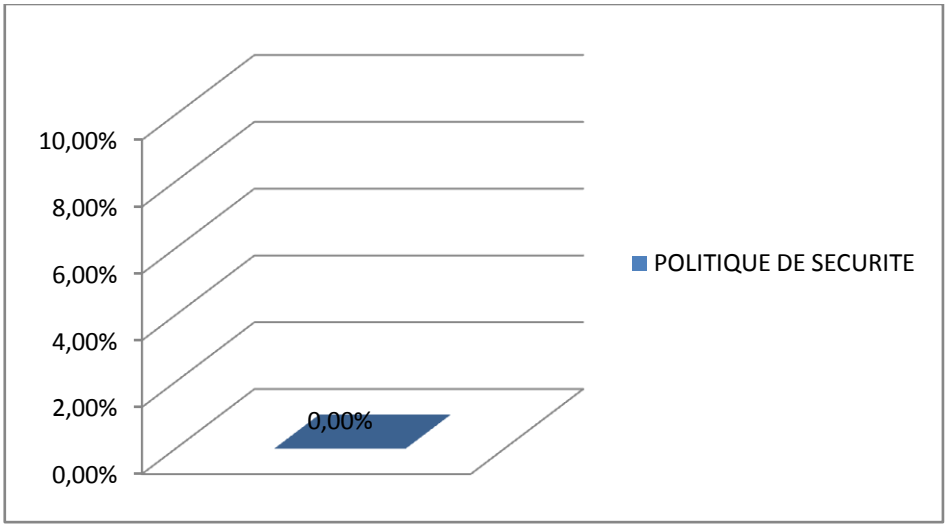
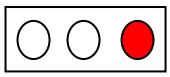


Figure 4.2 : Résultat des questions du domaine N°5 politique de sécurité

Observation

Selon cette représentation graphique, on observe que la politique de sécurité au sein de l'université de Guelma est nulle 0.00%.

Criticité



Constat

- l'absence d'une politique de sécurité formelle et disponible pour tous les personnels et par conséquent, le manque d'un document de politique de sécurité écrit, validé et diffusé par la direction générale et de norme appliquée.
- L'inexistence d'une politique de révision de la documentation pour l'organisation de la sécurité.

Recommandation :

- Etablir une politique de sécurité formelle et disponible pour tous les personnels.

5.2 Organisation de la sécurité d l'information :

Résultat

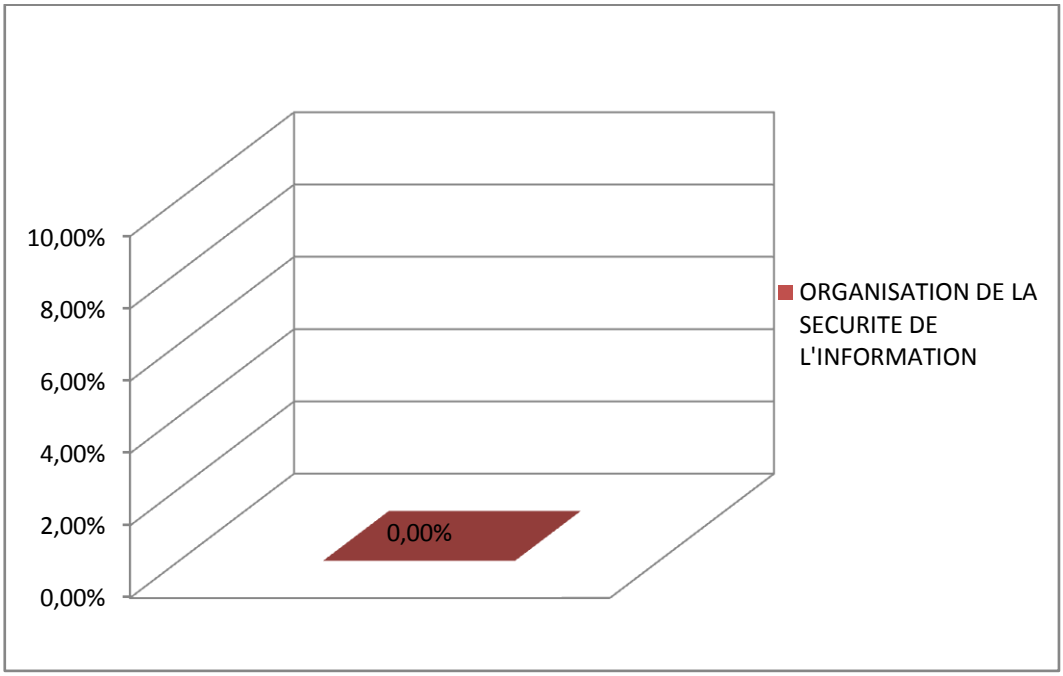
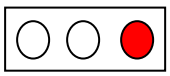


Figure 4.3 : Résultat des questions du domaine N°6 organisations de la sécurité de l'information

Observation :

Il n'y a aucune organisation de la sécurité de l'information selon ce graphe.

Criticité



Constat

- Le manque du management de la sécurité d'approche globale mais il y a des initiatives individuelles au niveau de faculté.
- L'inexistence d'une démarche méthodologique d'analyse et de gestion des risques SSI
- Les rôles et actions des différents acteurs de la SSI n'ont pas été définis pour faire l'objet d'une communication.
- L'Absence de l'identification des informations confidentielles.
- L'inexistence d'une révision périodique de la mise en œuvre de la gestion de la sécurité.
- L'Absence d'une politique de doublement du personnel clé de l'université
- L'existence des risques provenant des tiers (utilisateurs et sous-traitants)

- L'Absence de l'identification des risques dus aux tiers.

Recommandation :

- L'organisation de la sécurité consiste à Gérer, suivre et garantir la sécurité de l'information au sein de l'université de manière transversale.
- L'organisation de la sécurité consiste à définir les responsabilités et les rôles des différents acteurs de la sécurité.
- Assurer la sécurité de l'information et des moyens de traitement de l'information appartenant à l'université et consultés, communiqués ou gérés par des tiers.

5.3 Gestion des biens :

Résultat

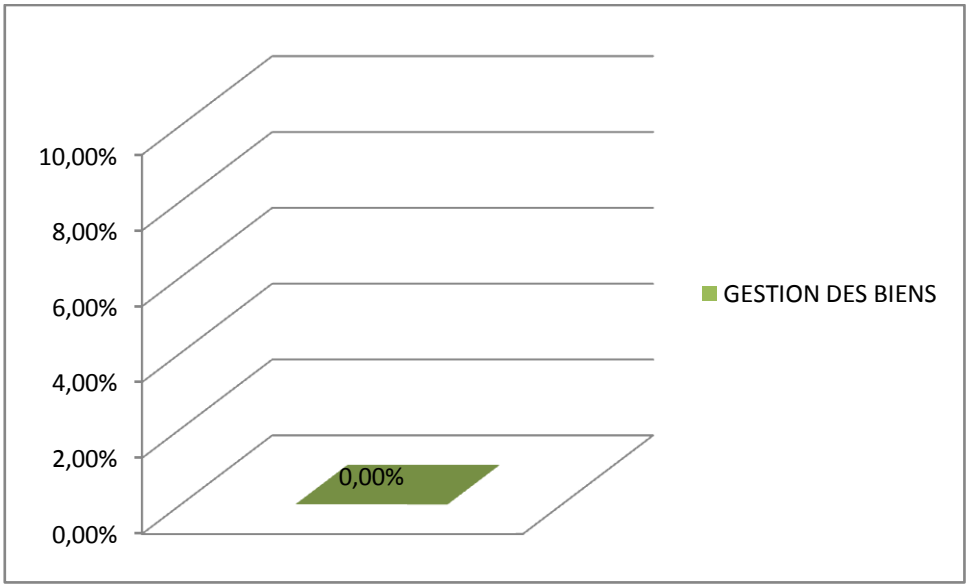
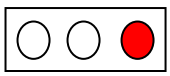


Figure 4.4 : Résultat des questions du domaine N°07 gestions des biens

Observation :

La gestion des biens est nulle (0.00%) selon cette représentation

Criticité



Constat

- L'inexistence d'un inventaire des biens de l'université au niveau du CCRSIC.
- L'Absence d'une classification des ressources basées sur les 3 axes : Disponibilité, Intégrité et Confidentialité.
- L'inexistence d'une campagne de diffusion ou de sensibilisation des utilisateurs pour l'utilisation correcte des biens.
- Manque des Lignes directrices pour la classification des informations en termes de valeur, d'exigences légales, de sensibilité et de criticité.

Recommandation

- Mettre en place et maintenir une protection appropriée des biens de l'université.
- Garantir un niveau de protection approprié aux informations.

5.4 Sécurité liée aux ressources humaines

Résultat

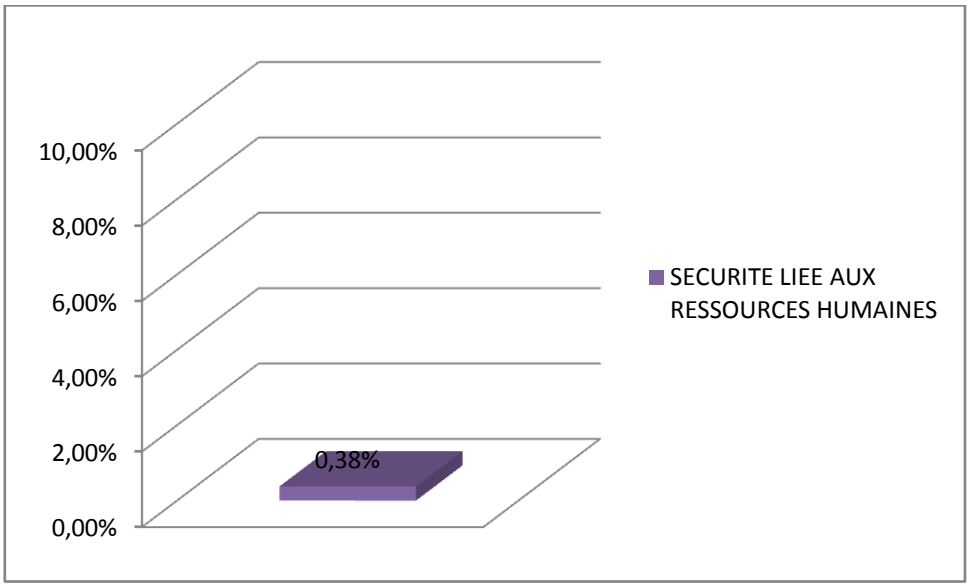
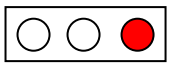


Figure 4.5 : Résultat des questions du domaine N°8 sécurités liées aux RH

Observation

La sécurité liée aux ressources humaines peut être estimée à 0.38 %, c.à.d. qu'elle est très insuffisante.

Criticité



Constat

- L'existence des critères standards, selon la règlementation, par rapport à la sensibilité des missions lors du recrutement d'une personne pour l'université.
- Le personnel temporaire n'appas les mêmes droits que les autres utilisateurs.
- Le contrat employeur employé, tient compte des responsabilités de l'employé vis-à-vis des biens de l'université mais ne tient pas compte des spécificités de l'utilisation des TIC.
- L'Absence d'une procédure d'apprentissage des accidents et des failles de sécurité.
- L'inexistence des procédures globale formalisées de retrait des droits d'accès des utilisateurs ainsi que des sous-traitants, cependant il existe une procédure non écrite concernant l'utilisation du SI de la scolarité.

Recommandation

- Définir une politique de sécurité concernant la gestion des ressources humaines.

5.5 Sécurité physique et environnementale

Résultat

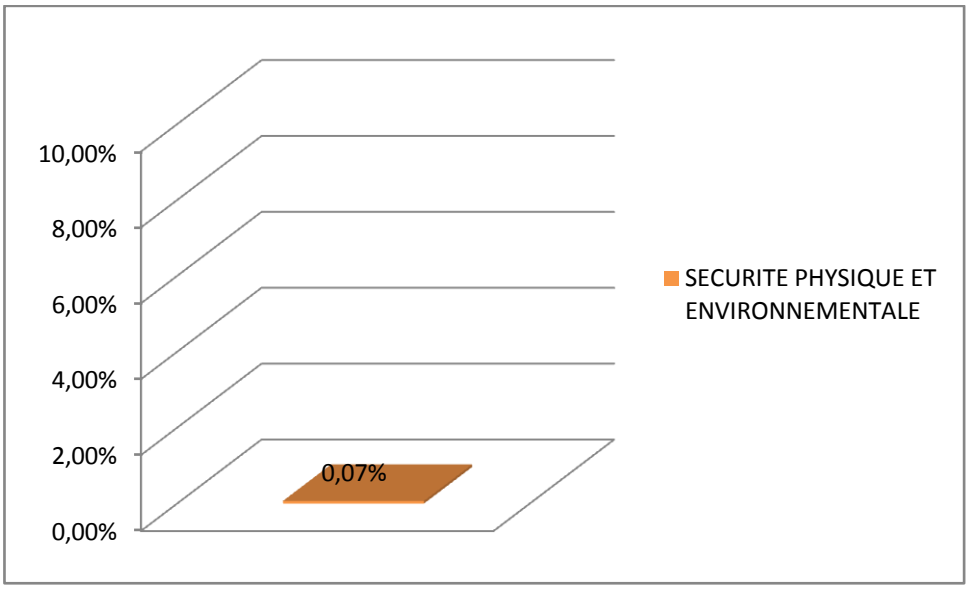


Figure 4.6 : Résultat des questions du domaine N°9 sécurités physiques et environnementales

Observation

On constate 0.07% de sécurité physique et environnementale des locaux et matériel informatiques de l'université, ce résultat présent uniquement l'existence d'un générateur électrique.

Criticité

Constat

- L'emplacement des locaux informatiques de l'université ne tient pas compte des
- L'absence de moyens de protection contre les risques naturels tels que : incendie, et la foudre, les inondations, etc. On a constaté par exemple l'inexistence de paratonnerre, de système de détection ou d'évacuation d'eau de système de détection d'incendie.
- L'inexistence d'un système de climatisation conforme aux recommandations du constructeur.
- L'absence d'une réglementation d'accès aux locaux informatiques.
- L'inexistence d'un document lié à la sécurité physique et environnementale.

- L'existence d'un générateur électrique.

Recommandation

- Les zones contenant des informations et des moyens de traitement de l'information doivent être protégées.
- Le matériel doit être situé et protégé de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.

5.6 Gestion des communications et de l'exploitation

Résultat

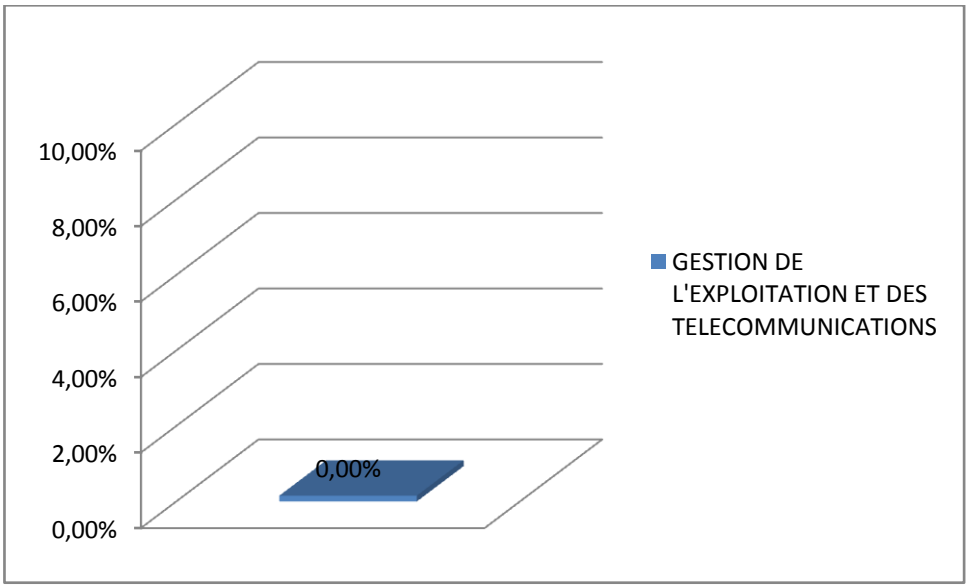


Figure 4.7 : Résultat des questions du domaine N°10 gestions de l'exploitation et des télécommunications

Observation

On constate 0 %de sécurité de gestion de l'exploitation et des télécommunications

Criticité

Constat

- L'absence des procédures formelles pour les opérations d'exploitation.
- les modifications de configuration ou de version n'ont pas fait l'objet d'un plan de conduite de changement appliqué au système.
- L'inexistence des procédures formelles pour la prévention contre la détection et la prévention des logiciels malicieux.
- L'absence d'une procédure pour la gestion des incidents.

- L'inexistence de procédures qui régissent les échanges des informations avec l'extérieur de l'université.
- L'absence d'une politique pour de destruction des documents officiels non utilisés.
- L'inexistence des consignes interdisant l'utilisation des logiciels sans licence qui doivent être respectés et contrôlés.
- L'absence d'une politique de traçabilité au sein de l'université
- les moyens mis en place afin de s'assurer du non répudiation d'une action se trouvent uniquement au niveau de la scolarité.
- L'inexistence des outils de centralisation et de journalisation des fichiers de journalisation.
- L'absence d'un partitionnement du réseau local en zone d'activité interne et une zone de communication avec l'extérieur.
- L'inexistence de vérification de la charge moyenne de chaque segment de réseau, la compatibilité du réseau et de ses équipements avec cette charge et cette vérification est régulièrement réactualisée
- Tous les équipements du réseau sont couverts par un contrat annuel de maintenance.
- L'absence d'une procédure de gestion des incidents du réseau local.

Recommandation

- Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.
- Suivre les événements systèmes et assurer le bon fonctionnement des SI.
- Détecter et analyser un dysfonctionnement
- Protéger l'intégrité des logiciels et de l'information.
- Contrôler et filtrer l'accès internet
- Maintenir l'intégrité et la disponibilité des informations et garantir leur restauration.

5.7 Contrôle d'accès

Résultat

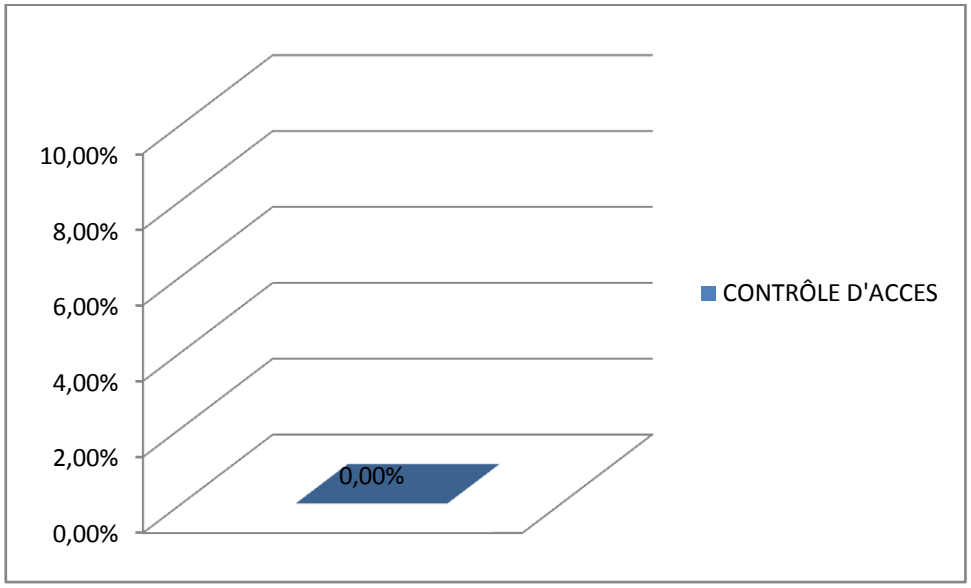
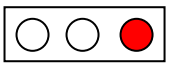


Figure 4.8 : Résultat des questions du domaine N°11 contrôles d'accès

Observation

On constate 0% de politique de contrôle d'accès sauf des initiatives individuelles au niveau SI de scolarité.

Criticité



Constat

- L'inexistence d'une politique de contrôle d'accès formalisée à l'exception du SI de la scolarité.
- L'absence d'une procédure de mis en place d'enregistrement d'un nouvel utilisateur.
- L'inexistence d'une procédure d'attribution des mots de passe.
- Les bonnes pratiques d'utilisation de mots de passe ne font pas l'objet d'une sensibilisation des utilisateurs. Sauf au niveau de la scolarité.
- L'absence des connexions au sein de l'université depuis l'extérieur.
- Les accès au SI ne sont pas soumis à des procédures sécurisées sauf au niveau de la scolarité.

Recommandation

- Une politique de contrôle d'accès doit être établie, documentée et réexaminée sur la base des exigences d'exploitation et de sécurité.

5.8 Acquisition développement et maintenance des systèmes d'information

Résultat

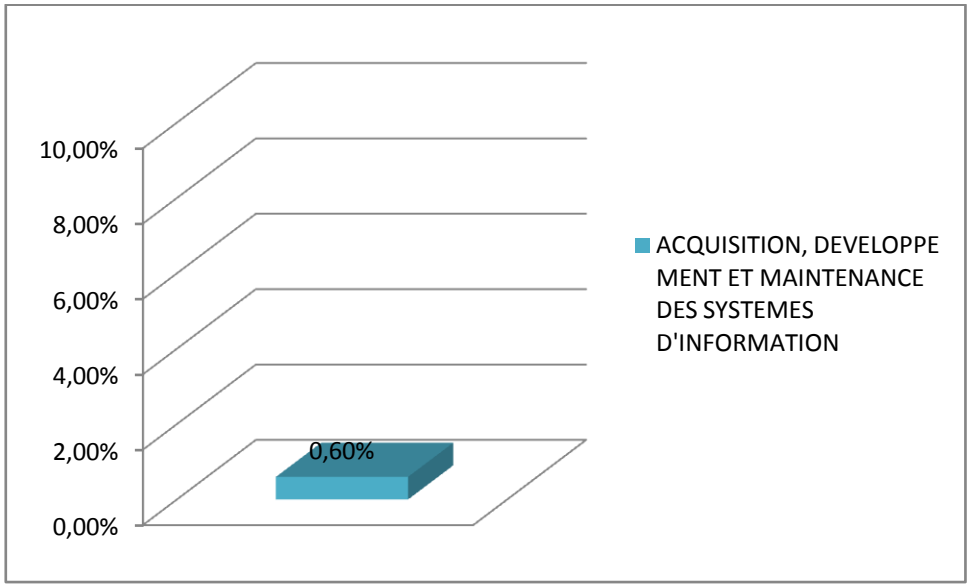


Figure 4.9 : Résultat des questions du domaine 12 acquisition ; développement et maintenance des SI

Observation

On constate 0.6% de sécurité de l'acquisition, développement et maintenance des systèmes.
Ce résultat présente :

- ✓ L'existence des mesures informatiques et administratives permettant à un utilisateur de vérifier l'authenticité et l'intégrité des informations mises à disposition.
- ✓ Il y a une prise en compte des risques de vol et fuite d'information.

Criticité

Constat

- L'existence des mesures informatiques et administratives permettant à un utilisateur de vérifier l'authenticité et l'intégrité des informations mises à disposition.
- Il y a une prise en compte des risques de vol et fuite d'information.
- L'absence d'une politique de gestion de clés d'accès aux applications. (responsabilités, procédures).

Recommandation

- La sécurité des informations doit être pris en compte dans le cycle de développement des systèmes les procédés de spécification, de construction / acquisition, les essais, la mise en œuvre et maintenir des systèmes informatiques.

5.9 Gestion des incidents lies a la sécurité de l'information

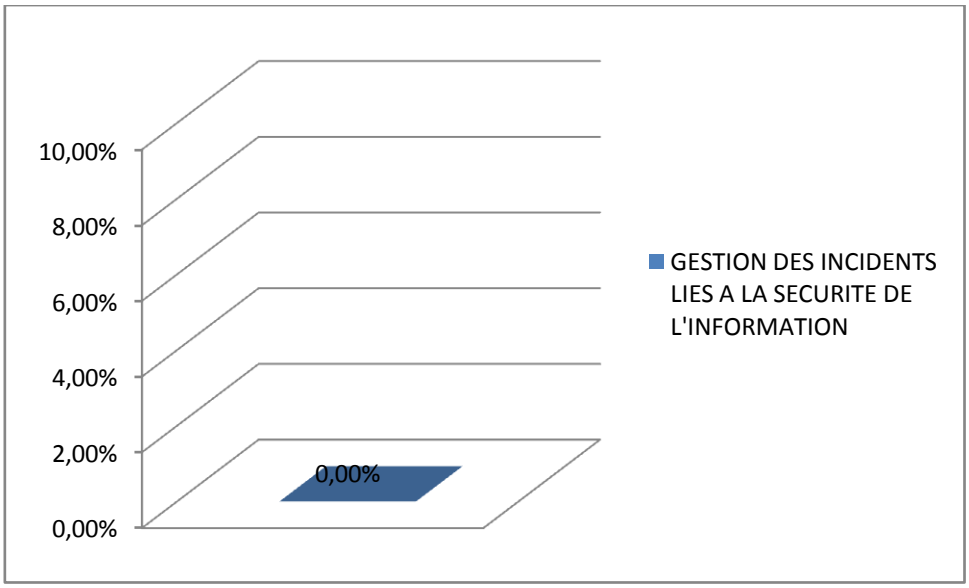
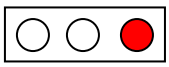


Figure 4.10 : Résultat des questions du domaine N° 13 gestions des incidents lies a la sécurité de l'information

Observation

On constate 0% de Gestion des incidents liés à la sécurité de l'information

Criticité



Constat

- L'inexistence d'une cellule de veille d'alerte de sécurité.
- Manque des fiches créées en cas d'incident de sécurité.
- L'inexistence d'une procédure de gestion des incidents.

Recommandation

- Une politique de Gestion des incidents doit être établie.

5.10 Gestions du plan de continuité de l'activité

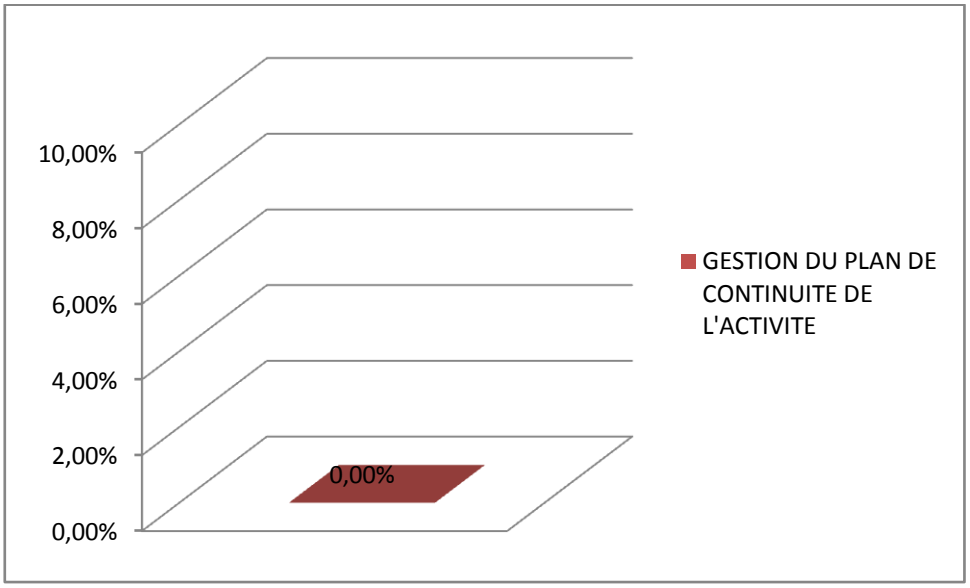
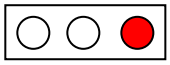


Figure 4.11 : Résultat des questions du domaine N°14 gestions du plan de continuité de l'activité

Observation

On constate 0% de Gestion du plan de continuité de l'activité

Criticité



Constat

- L'inexistence d'un plan ou une procédure de continuité d'activité

Recommandation

- Mettre en place un plan ou une procédure de continuité d'activité

5.11 Conformité

Résultat

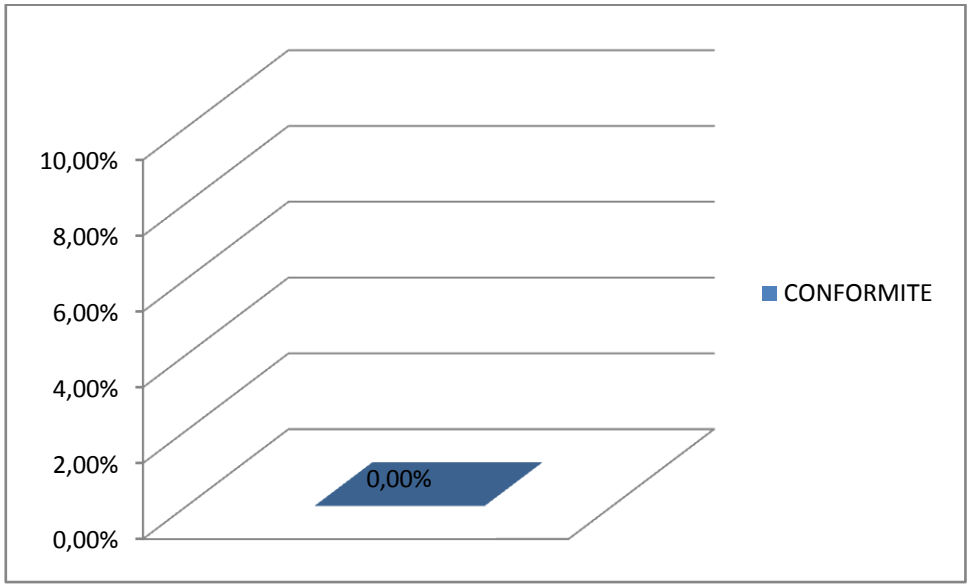
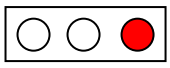


Figure 4.12 : Résultat des questions du domaine N°15 conformités

Observation

On constate 0% de conformité avec les exigences légales et les normes internationales de sécurité.

Criticité



Constat

- l'absence d'une définition, d'une documentation et d'une mise à jour explicite de toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences.
- L'inexistence d'une politique de sécurité qui précise qu'il est strictement interdit de posséder sur son poste tout logiciel non accompagné d'une licence en règle .

Recommandation

- Toutes les activités effectue par l'université doit être conforme avec les exigences légales et les normes international de sécurité.

6. Synthèse des résultats

Selon les résultats cités auparavant, nous assemblons les onze (11) thèmes de la norme ISO 27002 dans la même représentation graphique pour qu'on puisse constater et évaluer la politique et le niveau de la sécurité trouvaient dans l'université de Guelma grâce à l'opération d'audit réalisée.

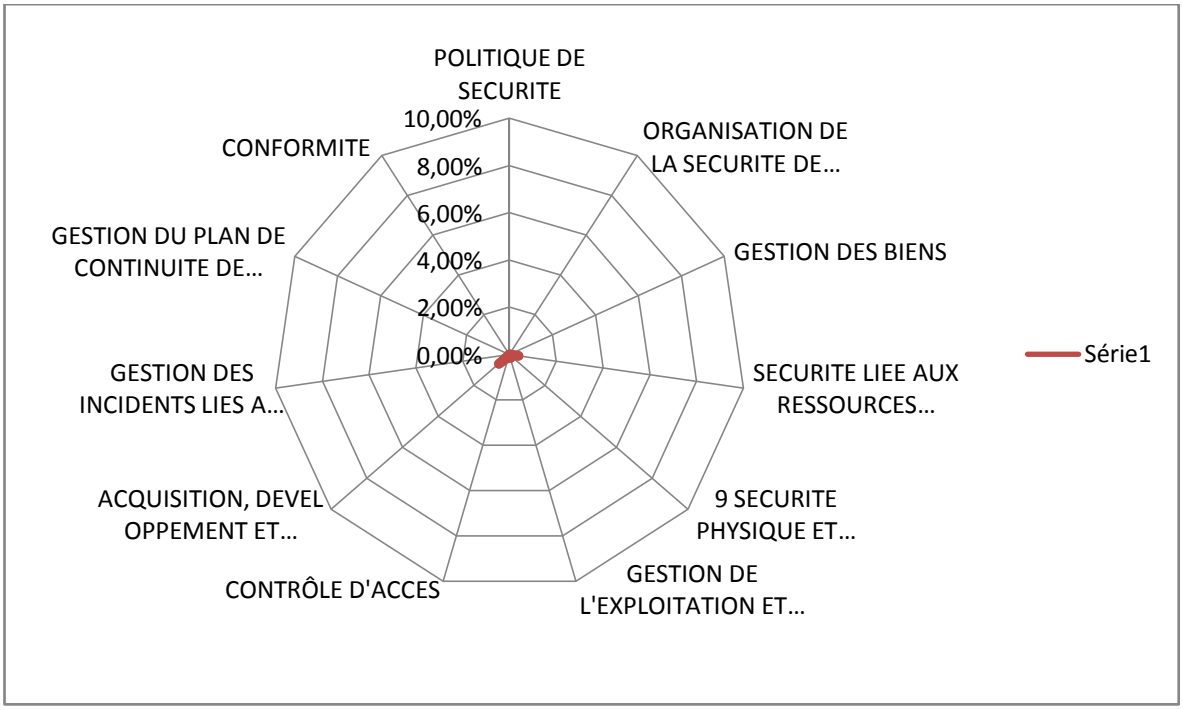


Figure 4.13 : Résultat des questions des onze (11) domaines de sécurité

D'une approche globale on constate que l'université ne possède pas d'une politique de sécurité formelle concernant les 11 domaines de sécurité de SI, sauf des initiatives individuel ; achats d'anti-virus ; logiciel de scolarité…

Conclusion

Durant cette partie, nous avons présenté l'essentiel de l'opération d'audit effectué au sein de l'université de Guelma. Prochainement nous définissons les règles de sécurité qu'il faut suivre.

Chapitre 5 : Les Règles de Sécurité pour l'Université de Guelma

Introduction

Après avoir évaluée la sécurité du système d'information suivant la norme 27002 au sein de l'université de Guelma, nous présentons dans ce chapitre l'ensemble des règles réparties par thème à mettre en œuvre pour pallier aux insuffisances constatées précédemment.

1 Organisation de la sécurité de l'information

On propose :

- Deux postes de responsable de sécurité des SI, pour assurer la continuité et la disponibilité des services.
- Un comité d'organisation de la sécurité de l'information (COSI), qui se compose du : CCRSIC, de deux responsables de sécurité, et un chef section réseau et un chef section application et un chef section Learning.

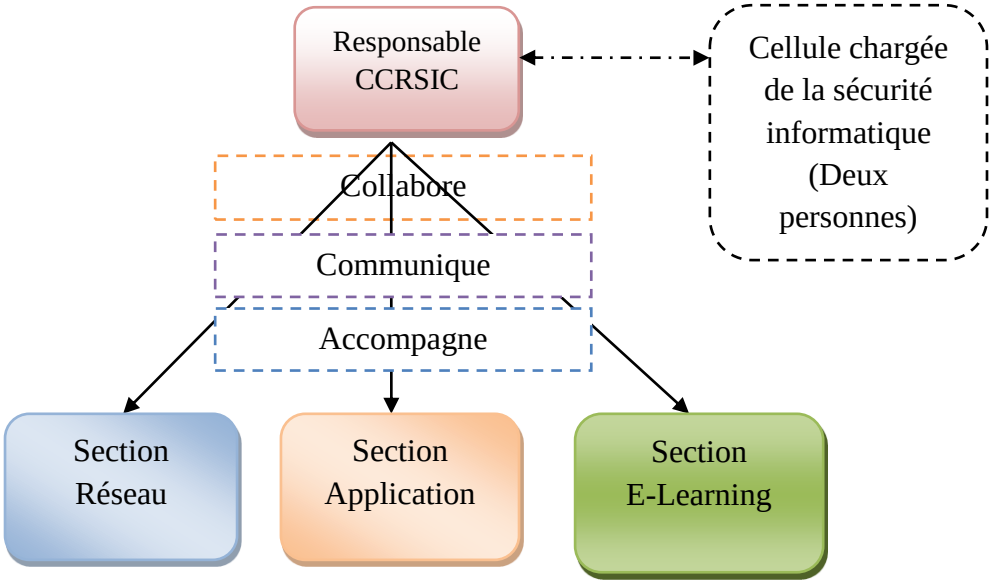


Figure 5.1 : Rattachement de la cellule chargée de la sécurité informatique dans l'organigramme du CCRSIC

1.1 Le Comité d'Organisation de la Sécurité de l'Information (COSI)

- Le COSI est chargé de la définition, de l'approbation, de la communication et de l'évolution de la PSSI.
- Le COSI produit et valide un plan de communication de la PSSI et de ses règles de

sécurité.

- Le COSI est en charge de gérer les exceptions (événement non pris en compte dans la PSSI) ayant un impact sur la sécurité des Systèmes d'Information de l'université.
- Le COSI a également pour objectif d'effectuer des retours d'expérience et d'échanger sur les pratiques de chacun dans le domaine de la sécurité des Systèmes d'Information.

Dans l'objectif de gérer la sécurité de manière transversale au sein de l'université, le RSSI rencontre régulièrement les différents responsable du COSI. Il s'agit de réaliser régulièrement un point d'avancement sur les projets sécurité relatifs à leur périmètre d'activité et d'échanger sur les pratiques de sécurité mises en place.

Des indicateurs transversaux de suivi d'avancement des projets de la PSSI sont complétés et approuvés par l'ensemble des membres du COSI.

Le COSI dispose d'un espace d'échange interne permettant d'assurer une communication transversale et un partage d'information optimal entre les sections (problèmes, incidents, vulnérabilité, …etc.

1.2 Gestion de crise

Le processus et l'organisation de gestion de crise sont identifiés localement au niveau de chaque entité, mais également au sein du COSI en cas de crise transverse. Ce document décrit comment les entités informatiques de l'université doivent réagir face à une crise, et cela de façon rapide et cohérente en utilisant une communication simple et transparente, dénuée de tout jargon informatique.

- Le Responsable Sécurité des Systèmes d'Information (RSSI) de l'université est désigné par la définition de sa fiche de poste précisant son périmètre d'action, ses responsabilités et ses moyens d'action. Il veille à la sécurité des Systèmes d'Information conformément à des grandes orientations et priorités et dans un souci de qualité, d'efficience et de précision.
- Le RSSI a un rôle de coordination pour la mise en œuvre et l'application de la PSSI de l'université. Il n'intervient pas directement au niveau opérationnel en tant que maître d'œuvre des projets de sécurité, mais :
- coordonne la gestion quotidienne de la fonction Sécurité,
- participe à l'homogénéisation du niveau de sécurité,
- En collaboration avec les autres membres du COSI, le RSSI développe des contacts avec les spécialistes externes au l'université, afin d'assurer une veille technologique en

matière de protection des informations.

- l'assurance de la perte de personnes clés pour l'activité de l'université.

1.3 Les chefs de Sections

- Les chefs de Sections assurent la responsabilité de la sécurité dans leur périmètre technique ou leur entité. Ils veillent au quotidien à l'application des procédures de sécurité pour la partie technique de l'exploitation systèmes, réseaux, postes de travail et applicatifs. Ils sont responsables de la mise en œuvre de la PSSI et du plan d'action sécurité dans leur périmètre.
- Ils assurent une veille sécurité (faille de sécurité, vulnérabilité, exploitations de vulnérabilités, etc.) en fonction de leur périmètre d'intervention afin de garantir le maintien du niveau de sécurité (poste de travail, système, réseau, etc.).

1.4 Gestion des tiers de chacune des entités :

- Les risques doivent être évalués par le RSSI ou les chefs de sections en question préalablement à la collaboration avec un tiers afin de déterminer les impacts sécurité et les mesures nécessaires lorsque l'université doit :
  - ✓ Collaborer avec des tiers et leur autoriser l'accès aux informations ou aux moyens de traitement (accès aux bureaux, salles des machines, dossiers papiers, accès logique interne ou externe), obtenir un produit ou un service d'un tiers, ou lui fournir un produit ou un service.
  - ✓ L'accès aux tiers ne doit être autorisé qu'aux systèmes utiles à la réalisation de leur travail dans la limite des attributions de chacun. La procédure d'accès est validée par tous les responsables de la COSI.
  - ✓ Tous les contrats avec des tiers doivent comporter un volet sécurité qui précise les règles de la PSSI d'université. Ce volet devra notamment mentionner l'obligation de faire signer un engagement de responsabilité et de confidentialité à leur personnel devant accéder à des données sensibles.
- L'université confie à des tiers la gestion et le contrôle de toute ou partie de son système d'information, de son infrastructure de traitement de l'information (réseaux, postes de travail, …etc.), il intègre dans le contrat de sous-traitance ses exigences de sécurité, à savoir :
  - ✓ le respect des exigences légales, dont la protection des données à caractère personnel,
  - ✓ les responsabilités en matière de sécurité pour l'Organisation et pour le sous-

traitant,

- ✓ la vérification du respect des exigences de confidentialité et d'intégrité des informations,
- ✓ les mesures de contrôle d'accès physique et logique à mettre en place et à respecter,
- ✓ les mesures de continuité de service en cas de survenance d'un sinistre,
- ✓ le niveau de protection physique des matériels confiés à des tiers,
- ✓ le droit d'audit de l'application des procédures et des installations de sécurité

2 Politique de sécurité de l'information

- ➢ La PSSI, approuvée par le COSI, est publiée et diffusée auprès de l'ensemble des salariés et des tiers concernés.
- ➢ La PSSI s'applique à l'ensemble des utilisateurs des Systèmes d'Information.
- ➢ Le document PSSI est revu à intervalle régulier par le COSI.
- ➢ La PSSI est systématiquement réexaminée à chaque changement organisationnel de l'activité ou de l'environnement technique.
- ➢ Un plan d'action est établit après réexamen afin de combler les écarts.
- ➢ La PSSI, pour chaque entité, un responsable (RSSI ou référent sécurité) de sa mise en œuvre, de son suivi et de son évolution. Il assure l'examen périodique de la mise en œuvre de la politique de sécurité en termes :
  - ✓ d'amélioration des dispositifs de sécurité des Systèmes d'Information, de diminution des incidents et de leurs impacts sur le fonctionnement de l'établissement (diminution des arrêts, diminution des pertes de données...),
  - ✓ de prise en compte de l'évolution des activités et de l'Organisation, ainsi que des nouveaux risques pesant sur les Systèmes d'Information de l'Organisation.
  - ✓ de mise au point des outils pour préserver l'intégrité des informations archivées.

3 Gestion des biens

- ➢ Chaque entité établit un inventaire des biens et le met à jour régulièrement pour chacun de ses Systèmes d'Information. Chaque bien doit être clairement identifié et documenté (localisation...) conformément aux recommandations du COSI.
- ➢ L'ensemble des applications installé sur les postes de travail doit être suivi et maitrisé.

- Une cartographie des applications est formalisée et régulièrement mise à jour en fonction des nouvelles applications et de celles sortant du périmètre. Cette cartographie applicative est nécessaire dans le cadre de projets structurants, comme la mise en place du Single-Sign-On, un Plan de Continuité d'Activité ou tout autre projet en lien avec un ensemble d'applications.
- Les responsables des biens inventoriées présents dans le périmètre préconisé par le COSI, doivent clairement être identifiés, tout comme la personne chargée de mettre à jour des caractéristiques du bien et de maintenir des mesures de sécurité appropriées sur le bien concernée.
- Une classification qui attribue les besoins et priorités de protection est établie. Cette classification repose sur les 4 axes correspondant aux besoins en termes de Disponibilité, d'Intégrité, de Confidentialité et de Traçabilité (DICT). La classification des biens s'appuie sur la procédure opérationnelle de classification des biens.
- II convient de classifier les biens sensibles pour indiquer le besoin, les priorités et le degré souhaité de protection lors de leur usage.
- A tout bien, et en particulier toute information sensible, doit être associé sa classification de sécurité (sur les 4 axes DICT).

4 Sécurité liée aux ressources humaines

- Des vérifications des informations concernant tous les candidats (postulants, contractants ou utilisateurs tiers) doivent être réalisées conformément aux lois, aux règlements et à l'éthique. Elles doivent être proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.
- Les droits d'accès de l'ensemble des salariés, contractants et utilisateurs tiers à l'information et aux moyens de traitement de l'information doivent être supprimés à la fin de leur période d'emploi, ou modifiés en cas de modification du contrat ou de l'accord.
- Etablir une clause dans les contrats d'embauche ou dans le règlement intérieur, précisant l'obligation de respecter l'ensemble des règles de sécurité en vigueur.
- La violation de la politique sécurité et des procédures de sécurité de l'organisme par des employés devra être traitée au moyen d'un processus disciplinaire et les mesures correspondantes doivent être communiquées à tous les employés.

- Le responsable /personnel de sécurité doivent être formé aux nouvelles technologies.
- une procédure d'apprentissage des accidents et des failles de sécurité doit être établie.

5 Sécurité physique et environnementale

Nous proposons de construire un data center sécurisé et respecte les normes de protection.

Le data center « est un ensemble informatique composé, entre autres, de serveurs, pour objectif d'offrir un centre d'hébergement et de traitement des données hyper sensibles à de grandes entreprises internationales, d'un niveau de sécurité très élevé.» **[31]**.

Le data center doit être éloigné des autres services, comme il doit respecter les points suivants :

- ✓ Faire les portes et les fenêtres métalliques.
- ✓ Faire l'entrée (l'ouverture) des portes modernes (carte d'accès-emprunte-code….).
- ✓ Ne laissez pas les produits et les objets qui facilitent les incidents.
- ✓ Prévoir des extincteurs qui alertent aux incendies
- ✓ Le câblage à l'intérieur doit être couvert ou sous terrain.
- ✓ Il faut mettre des consignes claires à propos du fait manger, boire ou fumer dans les locaux informatiques.
- ✓ la construction du siège doit être en béton armée.

- Définir des procédures spécifiques de contrôle pour chaque type de prestataire extérieur au service amené à intervenir dans les bureaux (sociétés de maintenance, personnel de nettoyage, etc.) : port d'un badge spécifique, présence d'un accompagnateur, autorisation préalable indiquant le nom de l'intervenant,…
- mettre détecteurs d'humidité à proximité des ressources sensibles.
- Définir des procédures de gestion de crise en cas de long arrêt du système et de permettre la reprise du fonctionnement au moins partiellement (favoriser quelques machines sur d'autres).
- L'accès à ce service doit être autorise qu'aux fonctionnaires de ce service vu son importance.
- L'alimentation en électricité avec des disjoncteurs puissants.
- Installer des caméras de surveillance.
- Faites la climatisation avec des climatiseurs géants (24000/32000/60000).

- Affichez dès l'entrée le règlement : ne touches rien; Pas de téléphone; Défense de fumer…
- Choisir un endroit plus spacieux.

6 Gestion des communications et de l'exploitation

6.1 Procédures et responsabilités liées à l'exploitation

- Les procédures d'exploitation (système, réseau, poste de travail, application) sont formalisées, partagées et les responsabilités associées (suivi, approbation, mise à jour) sont définies.
- La documentation des Systèmes d'Information (architecture, fonctionnement, procédures) est sauvegardée et son accès est réservé au personnel habilité.
- Pour chaque système sensible, des cahiers d'exploitation doivent être formalisés et doivent comprendre: le suivi des mises à jour de logiciels; la modification de paramètres; Les erreurs systèmes et actions correctives prises.
- Les cahiers d'exploitation doivent faire l'objet de contrôles réguliers par rapport aux procédures d'exploitation.
- Le processus de modifications majeures des Systèmes d'Information (ouverture vers l'extérieur, modification de l'architecture, ajout d'une application critique) doit faire l'objet d'une analyse des risques et d'une validation du réfèrent sécurité associé.

6.2 Sécurité liée à l'exploitation

- Les équipements des Systèmes d'Information sont surveillés en temps réel. Les principales informations concernant la disponibilité des services, la charge système et les espaces disques sont consolidées. en cas de dysfonctionnement, une alerte est remontée au RSSI.
- Le traçage des événements (ou logs) sur les systèmes doit être activé partout où il est disponible et pertinent.
- Une norme concernant la mise en place des logs sur l'ensemble des systèmes est définie, elle permet de garantir leur exploitation dans le temps.
- La collecte et la conservation des traces doivent être faites de manière à permettre leur utilisation comme élément de preuve aussi probant que possible.
- Le processus de gestion des changements (mise à jour des correctifs et mise à jour de sécurité) est formalisé et mis en production sur l'ensemble des équipements systèmes, réseaux, des postes de travail et des logiciels.

- Les délais d'applications des changements / mises à jour mineurs et majeurs applicatifs et systèmes sont définis par le référent sécurité associé.
- Les matériels et systèmes obsolètes doivent être clairement identifiés et doivent faire l'objet d'une analyse des risques par le référent sécurité associé.

6.3 Protection contre les malveillances

- Tous les serveurs et postes de travail doivent être protégés et supervisés afin de garantir l'intégrité des informations (données, configuration, etc.).
- Chaque entité informatique possède un processus de traitement des infections. Elle réalise un reporting centralisant les statistiques d'infection, dont la fréquence est définie par le COSI, à destination du RSSI à du réfèrent sécurité de chaque entité.
- Les protocoles réseaux autorisés et non autorisés doivent être identifiés et mis en production sur les équipements de sécurité péri métrique et de réseaux internes permettant leur cloisonnement.
- Toute connexion distante (sites distants, bureaux extérieurs, tiers, etc.) doit être réalisée en utilisant une solution permettant le chiffrement des flux. La liste des flux réseaux entrant et sortant autorisés est formalisée. Tous les flux n'étant pas décrits dans ce référentiel sont interdits.
- Les connexions internet des utilisateurs sont filtrées et journalisées. Une liste des sites non autorisés est établie et remise à jour régulièrement par le réfèrent sécurité en charge de ces aspects.
- Ils foutent faire vérification de la charge moyenne et crête de chaque segment de réseau, la compatibilité du réseau et de ses équipements avec cette charge et cette vérification est-elle régulièrement réactualisée.
- Mettre on over un partitionnement du réseau local en séparant du réseau strictement interne les zones de communication avec l'extérieur (DMZ).
- (Une DMZ, ou zone démilitarisée, est une zone d'échange avec l'extérieur isolée du réseau interne par un pare-feu).

6.4 Sauvegarde

- Une politique de sauvegarde est formalisée et validée par les référents sécurité en charge de ces aspects. Elle prend en compte :

- ✓ le responsable de la sauvegarde,
- ✓ la fréquence,
- ✓ Le type (complète, incrémentale, différentielle),

- ✓ le support (bande, disque),
- ✓ la durée de rétention,
  - ➢ des tests réguliers de restauration d'une sauvegarde / contrôle de l'intégrité des données sauvegardées
  - ➢ Les données sauvegardées doivent être délocalisées dans un local sécurisé distant de l'environnement de production.
  - ➢ La politique de sauvegarde est régulièrement revue et mise à jour par le RSSI ou le référent sécurité de chaque entité et les responsables des sauvegardes.
  - ➢ La politique de sauvegarde est communiquée de manière synthétique aux agents de l'université

6.5 Sécurité de l'information et des supports

- ➢ Les propriétaires d'information doivent définir les profils d'accès aux informations. Ces profils doivent distinguer les droits en lecture seule ou en lecture/écriture.
- ➢ Les utilisateurs doivent être sensibilisés à la mise en œuvre d'un ensemble de bonnes pratiques concernant les protections des documents physiques sensibles, par exemple :
  - ➢ ne doivent être sortis que les documents utiles,
  - ➢ quand ils ne sont plus utilisés, ils sont enfermés dans des armoires ou des coffres forts adaptés au niveau de sécurité requis,
  - ➢ la destruction est réalisée au moyen de destructeurs de documents / broyeurs,
  - ➢ les documents sensibles ne sont pas laissés sur les imprimantes réseau sans surveillance,
  - ➢ les fax sont immédiatement récupérés.
- ➢ Le processus de restitution des biens est formalisé, il prévoit la remise de l'ensemble des biens appartenant à l'université et, sauf en cas de demande de sa hiérarchie, la suppression des données présentes sur l'ensemble des supports.
- ➢ Lors du remplacement ou de la mise à la réforme des appareils de type fax, copieur, etc., les supports de stockage qu'ils contiennent doivent faire l'objet d'une gestion particulière, notamment pour ce qui concerne l'effacement sécurisé des données.

6.6 Archivage

L'environnement adapté à la gestion correcte des archives est défini par la politique d'archivage de l'université. Elle définit les responsabilités du Secrétariat général en matière d'archivage et établit des règles de base.

7 Contrôle d'accès

- L'identification de la personne se connectant au réseau est effectuée de façon formelle et non ambiguë. L'ensemble des utilisateurs des Systèmes d'Information (interne, tiers, etc.) possède un compte nominatif.
- Toute création, modification et clôture de compte (utilisateur, administrateur, service, etc.) doit pouvoir être suivie, tracée par le RSSI ou le référent sécurité de l'entité.
- L'ensemble des accès aux Systèmes d'Information est tracé.
- La collecte et la conservation des accès doivent être faites de manière à permettre leur utilisation comme élément de preuve.
- Les habilitations et les droits « utilisateurs avec pouvoir » sont répertoriés dans un référentiel (comptes nominatifs et comptes de service).
- La procédure des mouvements (arrivée, départ ou mutation interne), est formalisée et inclut la mise à jour du référentiel et des droits d'accès associés. Elle prend en compte le profil et la durée de la mission du nouvel utilisateur (interne ou tiers).
- Une politique de mots de passe complexe d'accès ciblant l'ensemble des utilisateurs des SI (internes, tiers) et les comptes de services est établie, respectant les préconisations relatives à la sécurité :
    - Processus de remise du mot de passe,
    - Longueur minimale,
    - Limite de tentatives d'accès,
    - Renouvellement.
- Des dispositifs limitant dans le temps les autorisations d'accès doivent être mis en œuvre pour assurer la protection de l'accès aux Systèmes d'Information:
    - ✓ économiseur d'écran activé et protégé par mot de passe,
    - ✓ encourager l'utilisation du verrouillage manuel quand l'utilisateur quitte son poste de travail,
    - ✓ arrêt du poste de travail en fin de journée.
- Les textes réglementaires sur l'accès aux documents du l'université sont régulièrement maintenus à jour par les Archives Centrales. L'accès aux systèmes d'exploitation doit être soumis à une procédure sécurisée d'ouverture de session.
- Les sessions inactives doivent être déconnectées après une période d'inactivité définie.

8 Acquisition, développement et maintenance des systèmes d'information

- Les développements et les acquisitions doivent prendre en compte les besoins des métiers en matière de sécurité. Une analyse des besoins de sécurité doit être effectuée suivant l'échelle des besoins de sécurité.

- Le RSSI ou le référent de chaque entité, doit être intégré dans les projets et dans le processus de validation d'un cahier des charges lié aux SI, particulièrement pour les projets dits "sensibles.
- Des audits de vulnérabilité des applications, bases de données et systèmes sensibles sont réalisés :
    - dans le cadre de leur mise en place,
    - à intervalle régulier,
    - en cas d'évolution majeure du système d'exploitation, de l'application ou de la configuration matérielle,
    - en cas d'apparition d'une nouvelle vulnérabilité majeure, dans le but de confirmer ou rejeter son exploitabilité.
- Un guide décrivant les bonnes pratiques et les règles de l'art pour les développements internes est formalisé par le référent en charges de ces aspects.
- Le processus de mise en production d'une application ou d'un système est formalisé. Il décrit l'ensemble des étapes du processus et spécifie que les différents environnements (développement, pré production, production) doivent être séparés.

9 Gestion des incidents lies a la sécurité de l'information

- Les responsabilités et les procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information doivent être établies.
- nous allons étudier la gestion des incidents en détail dans le chapitre six(06).

10 Gestions du plan de continuité de l'activité.

- Chaque entité met en place des Plans de Secours Informatiques et un Plan de Continuité d'Activité en accord avec les objectifs des métiers de l'Organisation.
- Les besoins en termes de secours informatique et de Continuité d'Activité, à savoir le Délai Maximal d'Interruption Tolérable (DMIT) et les Pertes de Données Maximales Acceptables (PDMA), doivent être intégrés dans les nouveaux projets

  Nous allons aborder ce domaine en détail dans le chapitre six (06)

11 Conformité

- Toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences doivent être explicitement définies, documentées et mises à jour.
- L'utilisateur doit accepter un message de mise en garde avant d'accès aux données sensibles dans tous les l'logiciel**.**
- une politique de sécurité doit être établie pour précise qu'il est strictement interdit de posséder sur son poste tout logiciel non accompagné d'une licence en règle .

Conclusion

Dans cette partie, nous avons proposé des règles que nous jugeons nécessaires à mettre en œuvre pour améliorer la sécurité du système d'information de l'université de 8 mai 1945 en se basant sur la norme 27002.

Chapitre 06 : Gestion des Incidents et plan de continuité de travail du SSI

Introduction

Ce chapitre présent un plan d'action pour la gestion des problèmes qui touche la sécurité de systèmes d'information de l'université, le premier s'articule autour de la gestion d'incidents au niveau de ce système, par contre le deuxième gère la continuité du travail de ce même système.

1 Gestion des incidents

1.1 Définition d'ISSI

Le ISSI peut être défini comme est tout évènement potentiel ou avéré, indésirable et/ou inattendu, impactant ou présentant une probabilité forte d'impacter la sécurité de l'information dans ses critères de Disponibilité, d'Intégrité, de Confidentialité et/ou de Preuve **[32]**.

1.2 Les étapes de la Gestion des incidents

- On propose une Équipe d'intervention en cas d'incident informatique

  CIRT :(*Computer Incident Réponse Team*).

- **Indentification des parties prenantes** :

Pour mieux gérer les incidents :

- un CIRT doit identifier ses parties prenantes, qui sont les entités dont les incidents sont traités par le cette équipe. On peut identifier une partie prenante par:
  - ✓ Les plages d'adresses IPv4 et IPv6
  - ✓ Le(s) numéro(s) de Système Autonome (AS)
  - ✓ Les nom(s) de domaine
- le personnel chargé de la sécurité doit exécuter à la lettre les étapes suivantes afin de minimiser au maximum les dégâts qui peuvent être provoqués par cet incident, la figure suivante nous montre l'ensemble

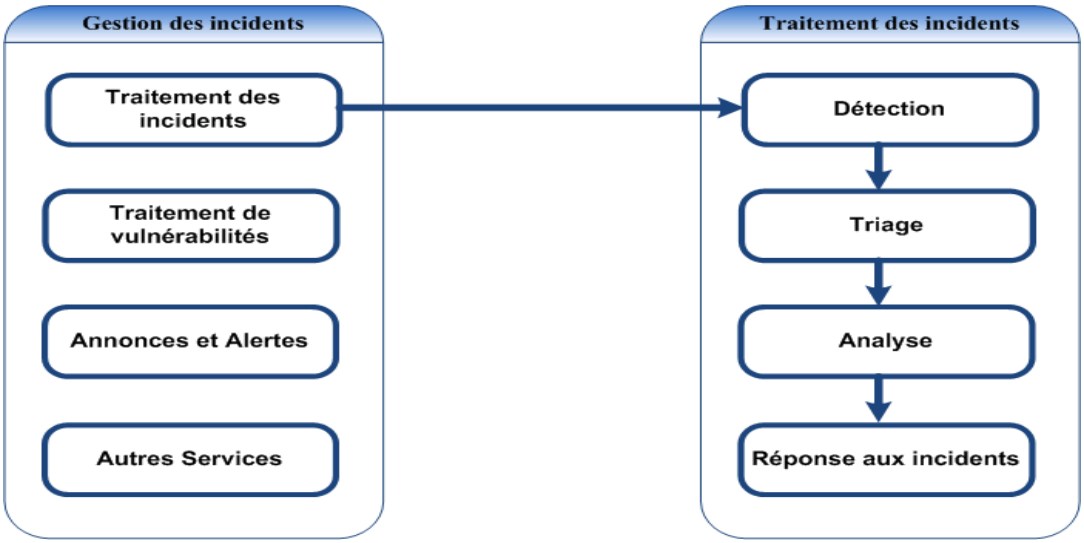


Figure 6.1 : Processus de gestion de traitement des incidents

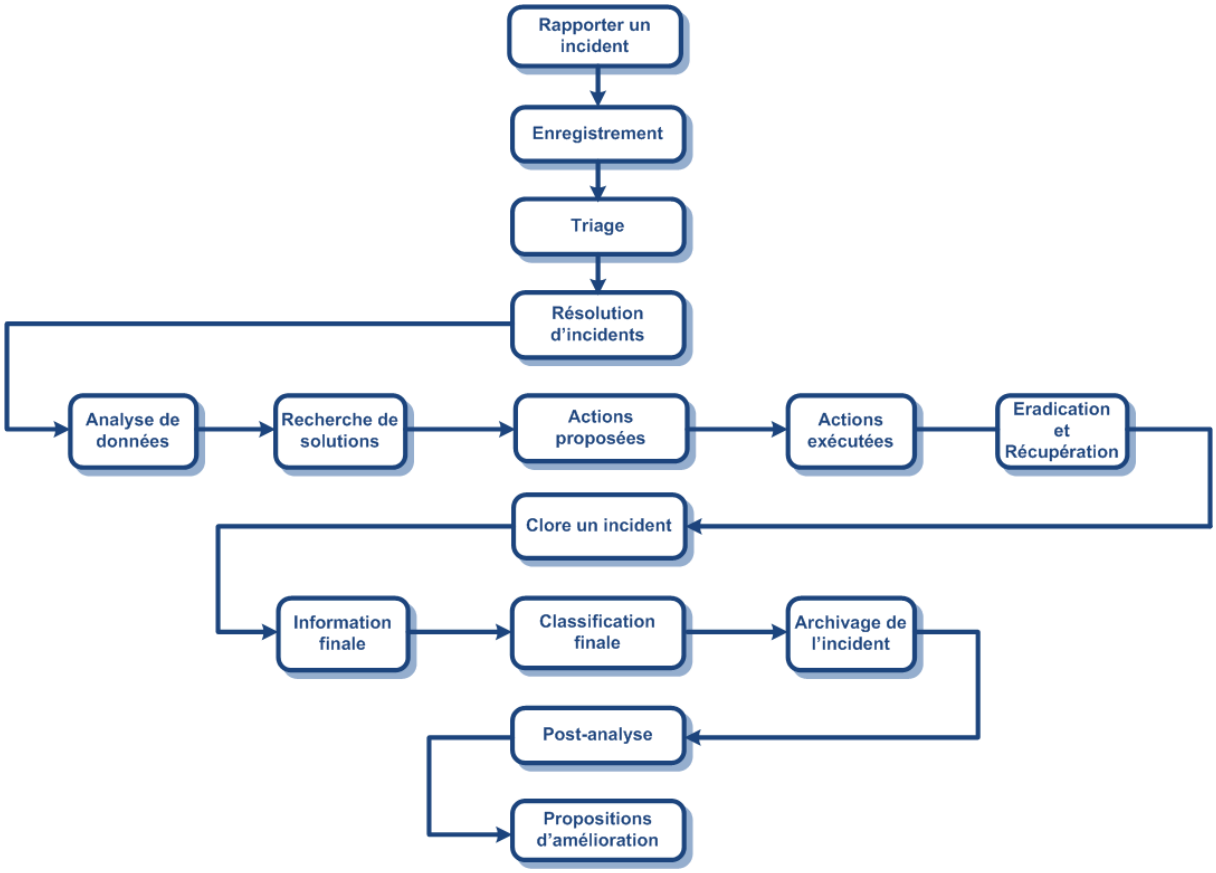


Figure 6.2: Flot de traitement d'incident

1.2.1 Rapporter un incident

- **Communication avec le CIRT**
  - ✓ Pour des communications ne contenant pas des Informations sensibles, le CIRT utilisera des courriels non Chiffrés
  - ✓ Pour les communications sécurisées, les courriels chiffrés avec PGP ou le téléphone seront utilisés
- **Tâches de la partie prenante**
  - ✓ La partie prenante doit fournir des informations de contact
    - ❖ Nom et organisation
    - ❖ E-mail
    - ❖ Numéro de téléphone
  - ✓ L'adresse IP et le type d'incident (spam, scanning, Dos, etc.) doivent être précisés
  - ✓ Si l'incident concerne le scanning, joindre une partie des logs montrant le problème
- **Tâches de la partie prenante**
  - ✓ Si l'incident concerne un spam ou un malware, joindre une copie entière de l'entête du courriel considéré comme spam et malware
  - ✓ Si l'incident concernant l'hameçonnage (phishing), joindre l'URL
- Le CIRT reçoit un incident rapporté par une de ses parties prenantes via :
  - ✓ Courriel (e-mail)
  - ✓ Formulaire web
  - ✓ Téléphone
  - ✓ Fax

1.2.2 Enregistrement

- ✓ Un incident rapporté est automatiquement enregistré dans le système de traitement des incidents

1.2.3 Triage

Dans le processus de traitement des incidents, la phase de triage consiste en étapes:

- ✓ Vérification
- ✓ Classification initiale
- ✓ Assignation

1.2.3.1 Vérification d'un incident

- ✓ L'incident rapporté est-il un vrai?
- ✓ L'incident a-t-il été rapporté par une des parties prenantes?

1.2.3.2 Classification initiale d'un incident

- L'incident doit être classé selon le schéma de Classification ci-dessous :

Classes d'incidents	Types d'incidents	Description/Exemples
Contenu abusif 10	Spam	Abusif pourriel ou polluriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.
	Harcèlement	Discrédits, ou discrimination contre une personne d'un point de vue cyber
Code malicieux	Virus, Ver, Cheval de Troie, Spyware, Dialler	Logiciel intentionnellement introduit dans un système pour un but nocif. L'interaction d'un utilisateur est normalement nécessaire pour activer ce code.
Collecte d'informations	Scanning	Attaques qui consistent à envoyer des requêtes à un système pour découvrir ses failles. Ceci inclut également tout type de processus de test pour collecter des informations.
	Sniffing	Observer et enregistrer le trafic réseau (Ecoute)
	Ingénierie sociale	Collecte d'informations sur un être humain sans utiliser de moyens techniques (ex : mensonges, menaces,…)
Tentatives d'intrusion	Exploiter des Vulnérabilités Connues	Une tentative pour compromettre un système ou interrompre tout service en exploitant les vulnérabilités avec des identifiants standardisés comme un nom CVE
	Tentatives de Connexion	Tentatives de connexion multiples (vol ou crack de mots de passe, force brute).
	Signature d'une nouvelle attaque	Une tentative pour exploiter une vulnérabilité inconnue.
Intrusions	Compromission d'un compte privilégié Compromission d'un compte non privilégié Compromission d'une Application	Une compromission réussie d'un système ou d'une application (service). Ceci peut être causé à distance par une nouvelle vulnérabilité ou une vulnérabilité inconnue, mais aussi par un accès local non autorisé
Disponibilité	DoS DDoS	Dans ce type d'attaque, un système est bombardé avec une grande quantité de paquets

	Sabotage	que les processus deviennent lents ou que le système crache. Exemple d'un Dos distant : PING flooding ou des bombes E-mails (DDOS , Toutefois, la disponibilité peut aussi être affectée par des actions locales (ex : destruction, interruption d'alimentation électrique, …etc.).
Sécurité de l'information	Accès non autorisé aux informations. Modification non autorisée aux informations.	En plus d'un abus local des données et des systèmes,la sécurité de l'information peut être mise-en mal par un compte ou une application compromise. Aussi, les attaques qui interceptent et accèdent aux informations pendant leur transmission sont possibles (écoute, usurpation,).
Fraude	Usage non autorisé des ressources	L'utilisation des ressources à des buts non autorisés, incluant des activités à but lucratif (ex. l'usage d'email pour participer dans des transactions illégales.
	Droit d'auteur (Copyright)	Vendre ou installer des copies de logiciels commerciaux illégalement ou d'autres matériels sous droit d'auteur.
	Mascarade	Type d'attaques dans lequel, une entité assume illégitimement l'identité d'un autre dans le but de bénéficier de lui.
Autres	Tout incident qui ne fait pas partie des catégories citées ci dessus.	Si le nombre d'incidents dans cette catégorie croit, ceci indique que le schéma de classification doit être révisé.

Tableau 6.1 : Classification initiale d'un incident

- Beaucoup d'informations sont nécessaires à cette étape
- Un autre facteur à prendre en compte dans la priorisation est la sévérité de l'incident à traiter

➢ **Comment prioriser les actions entre les parties prenantes?**

- Pour un CIRT qui en fonction de sa mission, doit protéger l'administration publique et en plus un contrat avec des institutions financières pour la fourniture de services de traitement d'incidents.
- Dans ce cas, on doit diviser les incidents potentiels en trois groupes en fonction de leur sévérité.

Groupe	Sévérité	Exemple d'incidents	Temps De réponse
Rouge	Elevé	• Disponibilité • Code Malicieux • Intrusions	3heures
Orange	Moyen	• Tentatives d'intrusion • Sécurité de l'information • Fraude	24heures
Jaune	Faible	• Contenu abusif • Collecte d'informations	3jours

Tableau 6.2: La division des incidents potentiels selon leur sévérité

1.2.3.3 Assigner un incident

- Un incident est assigné au responsable du traitement d'incident
- Cette personne peut être celle qui est la première à prendre l'incident à partir de la boite de réception des incidents
- Une personne peut être spécialiste du traitement d'un incident donné (spam, malware)
- Un incident peut être assigné à une personne en fonction de sa disponibilité

1.2.4 Résolution d'incidents

La phase la plus longue pour la résolution de l'incident s'effectue selon le cycle suivant :

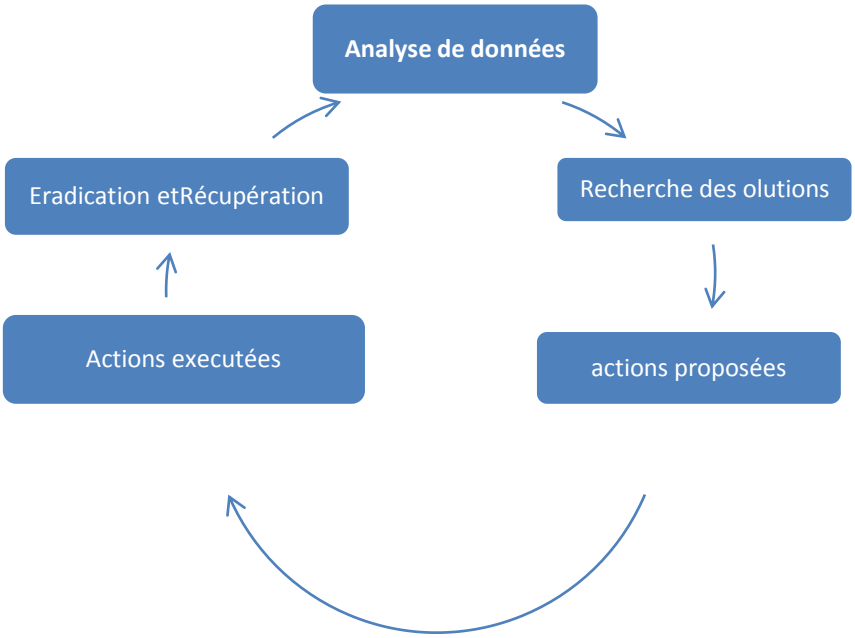


Figure 6.3 : Résolution d'incidents

1.2.4.1 Analyse de données

- Pour débuter l'analyse de données, les parties prenantes concernées seront contactées pour collecter plus d'informations sur l'incident
- Des conseils et informations initiaux seront inclus dans cette notification pour mieux orienter la résolution de l'incident

1.2.4.2 Recherche de solutions

- Les informations collectées pendant la phase d'analyse sont utilisées dans cette phase

1.2.4.3 Actions proposées

- Une liste de tâches concrètes et pratiques sont élaborées pour chaque partie prenante

1.2.4.4 Actions exécutées

- Les infrastructures des parties prenantes n'étant sous le contrôle du CIRT
- Le CIRT doit s'assurer que ces parties ont exécutées les actions proposées

- C'est la phase la complexe
- Le CIRT peut contacter les parties prenantes par mail, téléphone pour s'assurer de l'exécution des actions proposées

1.2.4.5 Eradication et récupération

- Toutes les actions auront pour seul but d'éradiquer les incidents
- La résolution réelle d'un problème est de restaurer un service Compromis dans son état normal

1.2.5 Clôture d'un incident

1.2.5.1 Information finale

- Après la résolution d'un incident, les parties concernées seront informées
- Deux questions à répondre ici :
  - ✓ Qui informer?
  - ✓ Informer sur quoi?
- Des indications sur les procédures de réduction des incidents seront fournies à ce niveau à chacune des parties prenantes

1.2.5.2 Classification finale

- ✓ Cette étape n'est pas obligatoire
- ✓ Elle survient à un niveau où des informations supplémentaires ne sont plus nécessaires

1.2.5.3 Archivage de l'incident

- ✓ Tout incident sera archivé et servir pour de futures Opérations

1.2.6 Post Analyse

- ✓ Très utile au CIRT dans l'optique de faire un bilan du traitement de l'incident

1.2.7 Propositions d'amélioration

- ✓ Le traitement d'incidents est un service réactif
- ✓ Il peut être en 1ère ligne pour des actions proactives et permettre des améliorations pour une bonne culture de sécurité
- ✓ C'est l'étape où il faut faire bénéficier de l'expérience de traitement d'incidents en fournissant des conseils et des recommandations aux parties prenantes

1.3 Approche détail de traitement d'incidents

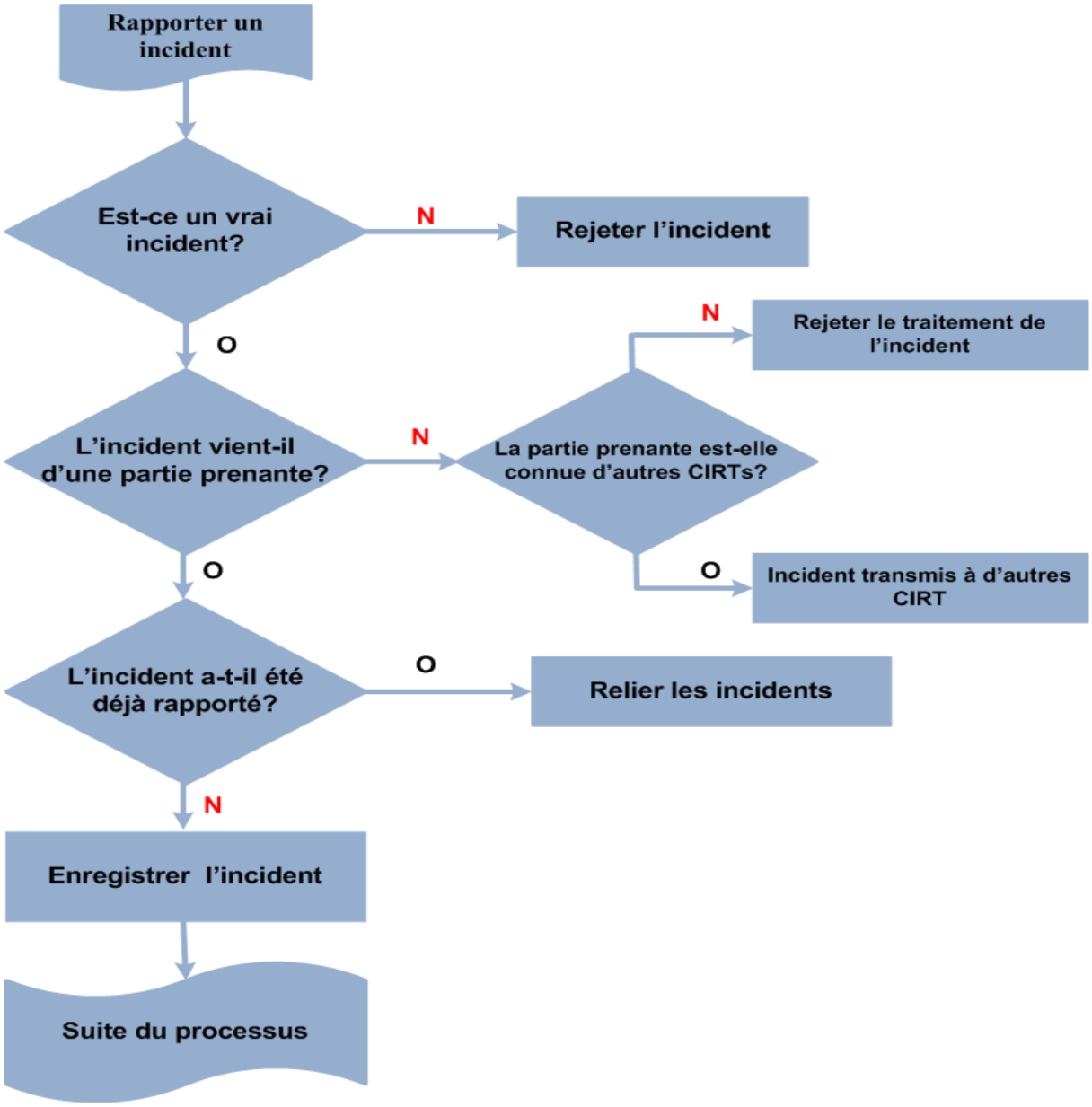


Figure 6.4 : Approche détail de traitement d'incidents

2 Le plan de continuité de l'activité (PCA)

2.1 Définition

Ensemble de mesures visant à assurer, selon divers scénarios de crises, y compris face à des chocs extrêmes, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise, puis la reprise planifiée des activités.

2.2 Organisation

Pour bien géré le PCA on propose une organisation de pilotage pour la mise en œuvre du secours.les différentes tâches de pilotage et de mise en œuvre du secours doivent être affectées à des « acteurs ». Ces acteurs sont des entités opérationnelles prédéfinies composées de personnes en nombre suffisant, de manière à ce que, en cas de sinistre, la réalisation de la tâche soit garantie.

Les premiers intervenants sont chargés d'appliquer les consignes et de donner l'alerte, selon les procédures d'escalade définies.

En cas de sinistre, on distinguera ensuite :

- le comité de crise ;
- la cellule de coordination ;
- les équipes d'intervention ;

On désignera également par « structure de crise » l'ensemble Comité de Crise-Cellule de Coordination.

2.2.1 Le Comité de Crise

Le comité de crise doit être composé au minimum des responsables suivantes : le responsable du CCRSIC, le responsable du SSI et le responsable des sections.

Le comité de crise prend les principales décisions concernant le secours. Il juge en particulier de l'opportunité de déclencher tel ou tel volet du Plan de Secours Informatique, en fonction du contexte. Le Comité de Crise peut se faire assister de compétences spécifiques, internes ou externes, notamment pour la communication et les aspects juridiques.

Des moyens de communication avec le comité de crise doivent être prédéfinis et garantis en cas de sinistre (lieu de réunion, numéros de téléphone, de fax, ...).

2.2.2 La Cellule de Coordination

Le pilotage proprement dit des opérations de secours peut être confié à une cellule de coordination, qui déchargera le comité de crise de tâches de coordination.

La cellule de coordination sera idéalement composée d'un petit nombre de personnes : le responsable du CCRSIC, le responsable du SSI. Certaines décisions peuvent être déléguées à cette cellule de coordination par le comité de crise, notamment l'anticipation du déclenchement de certains dispositifs (exemple : réservation du site de secours chez un prestataire).

2.2.3 Les équipe d'intervention

La réalisation des tâches de secours incombe aux équipes d'intervention définies selon les compétences requises, la disponibilité et le lieu d'intervention. On devra s'assurer que les contrats de travail sont compatibles avec un déplacement des équipes concernées sur un autre Exemples :

- équipe d'intervention informatique, composée d'un spécialiste réseau et d'un agent de maintenance, chargée des opérations sur le site de secours ;
- ingénieur de programmation
- équipe d'intervention réseau chargée du paramétrage réseau sur le site de secours des utilisateurs ;… etc.

Notons enfin que certains acteurs externes à l'entreprise doivent également être identifiés : prestataire de secours, fournisseurs d'énergie, opérateur téléphonie, fournisseur d'accès Internet, ...

L'ensemble des intervenants internes et externes avec leurs coordonnées doit être répertoriés dans un « annuaire du plan de secours » tenu à jour.

2.3 Étapes de plan de continuité de l'activité (PCA)

2.3.1 Déclenchement

La structure de crise est composée du comité de crise et de la cellule de coordination. Les procédures d'escalade sont essentielles. Lorsqu'un incident survient, la personne informée qui est souvent à un poste de sécurité de l'entreprise doit savoir qui contacter et comment contacter (notamment en cas d'indisponibilité des moyens habituels de communication). Cette personne doit à son tour, selon le type et la gravité de l'incident, connaître les personnes à contacter pour avoir des précisions ou bien mobiliser la structure de crise. Il est important de définir à l'avance qui est habilité à activer la structure de crise et surtout n'appeler que les personnes strictement désignées afin d'éviter un encombrement inutile des lignes.

2.3.2 Les dispositifs de secours

Un plan de secours est composé de dispositifs élémentaires (procédures techniques ou organisationnelles) dont l'activation dépendra de l'événement survenu et du contexte général.

Le déclenchement de certains dispositifs ou leurs modalités d'exécution peuvent en effet dépendre de nombreux éléments (exemple : la communication de crise).Les dispositifs d'un plan de secours peuvent être classés par types d'activité :

- La mobilisation des ressources nécessaires :
  - ressources humaines : mobilisation des équipes d'intervention ;
  - réservation des moyens de secours (réquisition de moyens, alerte d'un prestataire externe, ...) ;
  - récupération des sauvegardes ;
  - récupération de la documentation ;
- le secours des équipements informatiques :
  - restauration des environnements système ;
  - adaptations techniques (le matériel de secours n'est pas toujours identique au matériel d'origine) ;
  - restauration des applications ;
  - validation des restaurations ;
- le secours des réseaux :
  - mise en place des équipements de secours ;
  - basculement sur liaisons de secours ;
  - paramétrage des différents équipements ;
  - le secours de la téléphonie :
  - re-routage des appels ;
  - mise en place d'équipements de secours ;
  - paramétrage ;
- la reprise des traitements :
  - adaptations logicielles ;
  - adaptation des procédures d'exploitation ;
  - récupération de flux et synchronisation des données ;
  - traitements exceptionnels ;
  - validations fonctionnelles ;
- la logistique :
  - transports ;
  - fournitures ;
  - gestion de crise du personnel (choix des personnels à mobiliser, rotation des équipes, prise en compte des situations individuelles

- le relogement :
  - organisation du relogement d'urgence ;
  - préparation des sites d'accueil ;
- la reprise des activités des services utilisateurs :
  - tâches utilisateurs avant mise en place des moyens de secours ;
  - organisation d'un service minimum ;
  - travaux exceptionnels (procédures de contournement, rattrapages, ...) ;
- la communication de crise :
  - interne (personnel, autres entités, ...) ;
  - externe (clients, partenaires, public, ...) ;
- les dispositifs de post-reprise :
  - dispositifs préalables et d'accompagnement (assurance, remise en état des locaux, sauvetage des matériels, ...) ;
  - dispositifs de retour à la normale (constituent un plan spécifique).

Pour être opérationnels, ces dispositifs de secours doivent être accompagnés de dispositifs permanents destinés à les maintenir à niveau (exemples : le plan de sauvegarde, les procédures de mise à jour et de formation des acteurs du PSI, ...).

2.4 Documentation

La documentation constitue un élément essentiel d'un plan de secours. Elle est en général assez volumineuse et très évolutive (nouvelles affectations de personnel, évolution de configurations, nouvelles applications, ...). Pour toutes ces raisons, il est conseillé de gérer la documentation à l'aide d'un outil spécialisé dans la gestion de plans de secours ou de plans de continuité d'activité. On veillera également à la confidentialité de ces documents, susceptibles de contenir des informations stratégiques de l'entreprise et nominatifs. La documentation d'un plan de secours peut être structurée en 4 niveaux, selon l'objectif visé : communiquer, mettre en œuvre, gérer, contrôler.

2.4.1 Les documents de communication sur le plan de secours

La communication interne sur le plan de secours ne doit pas être négligée. Elle doit permettre aux différents responsables d'avoir une bonne vue d'ensemble des solutions prévues et de leurs conditions générales de mise en œuvre. Cette documentation inclura notamment :

- un rappel des objectifs de continuité de service ;
- une description générale des différents dispositifs du plan de secours (secours des

équipements informatiques, secours des télécommunications, solutions de relogement, communications de crise, ...) ;

- une description générale de la structure de crise ;
- les principes d'alerte de la structure de crise et de pilotage des opérations ;
- un rappel des risques résiduels.

2.4.2 Les documents de mise en œuvre du Plan de secours

Ces documents constituent le cœur du plan de secours. Ils sont destinés aux personnes ayant la responsabilité des différents dispositifs du plan et décrivent tous les éléments utiles à leur mise en œuvre : procédures, documentation technique, éléments de synchronisation, contrats, ... La documentation technique devra, par son niveau de détail, permettre de réduire les erreurs humaines liées au stress.

Concrètement, cette documentation comportera au minimum :

- un annuaire du plan de secours, répertoriant tous les intervenants potentiels, internes ou externes, avec leurs coordonnées ;
- une description de la stratégie de secours retenue pour chaque risque identifié. Ce document est destiné à la structure de crise pour l'aider dans ses décisions. La stratégie de secours définit l'ensemble des dispositifs de secours à déclencher selon le contexte de l'incident (type d'événement, étendue des dégâts, ...) ;
- le planning des différentes phases de reprise ;
- les fiches de tâches à réaliser, structurées par acteur et / ou dispositif de secours ;
- la « feuille de route » de chaque acteur du plan, pour chaque cas répertorié ;
- l'ensemble des annexes utiles (documents de procédures, documentation technique, copies de contrats, schémas, ...).

Associée à un outil de pilotage, cette documentation permettra également à la structure de crise le suivi du déroulement des opérations.

Un exemplaire de cette documentation (papier et / ou outils de gestion du plan) sera conservé à l'extérieur de l'entreprise, dans un lieu sécurisé dont l'accessibilité doit être compatible avec les objectifs de redémarrage.

2.4.3 Les documents de gestion du plan de secours :

Pour la gestion du plan de secours, il convient d'établir une documentation complémentaire destinée aux responsables du plan et des dispositifs associés. Cette documentation a pour but de faciliter les évolutions ultérieures. Elle peut être constituée de

tableaux d'analyse des ressources et de leur utilisation, de listes de diffusion des documents. Elle inclut également l'historique des résultats de tests et les plans d'ajustement consécutifs.

2.4.4 Les documents de contrôle du plan de secours

- Tableaux de bord :
  - Planning de tests ;
  - Compte-rendu détaillé des tests ;
  - Indicateurs de qualité des dispositifs et du plan ;

Evaluation des risques résidu

Conclusion

Dans ce chapitre, nous avons proposé les étapes de la gestion d'incidents et de plan de continuité de travail du système d'information de l'université. Et dans le dernier chapitre nous proposerons une charte destinée à l'ensemble du personnel et d'utilisateurs de ce système.

République Algérienne Démocratique et Populaire

Ministère e l'Enseignement Supérieur et de la Recherche Scientifique

Université 8 Mai 1945 Guelma

Centre commun de réseaux, de systèmes d'information et de la communication et de télé-enseignement

№ : …...**/CSI/CRSICT/UG/2015** **Guelma le :** ……..……

Charte du Bon Usage du Système d'Information

- Vu l'ordonnance n° 66-155 du 8 juin 1966, modifiée etcomplétée, portant **code de procédure pénale** ;
- Vu l'ordonnance n° 66-156 du 8 juin 1966, modifiée etcomplétée, portant **code pénal** ;

- Vu la loi n° 99-05 du 18 Dhou El Hidja 1419 correspondant au 4 avril 1999 portant **loi d'orientation sur l'enseignement supérieur** modifiée et complétée.

- Vu **l'ordonnance** n° 03-05 du 19 Joumada El Oula 1424 correspondant au 19 juillet 2003 **relative aux droits d'auteur et aux droits voisins** ;

- Vu l'ordonnance n°06-03 du 19 JoumadaEthania 1427 correspondant au 15 juillet 2006 portant **statut général de la fonction publique.**

- Vu la loi n° 08-09 du 18 Safar 1429 correspondant au25 février 2008 portant **code de procédure civile et administrative** ;

- Vu la **loi** n° 09-04 du 14 Chaâbane 1430 correspondant au 5 août 2009 portant règles particulières relatives à **la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication**.

- Vu l'arrêté interministériel du 8 Rajab 1425 correspondant au 24 août 2004 fixant **l'organisationadministrative du rectorat, de la faculté, del'institut, de l'annexe de l'université et deses services communs**.

- Vu le décret exécutif n° 12-273 du 08 Chaâbane 1433 correspondant au 28 juillet 2012, modifié et complété, le décret exécutif n° 01-273 du 30 Joumada El Thania 1422 correspondant au 18 septembre 2001, **portant création de l'université de Guelma.**

- Vu la délibération du conseil d'administration de l'université 8 Mai 1945, Guelma à mettre en place une politique de sécurité de son système d'information ;

Promulgue la charte dont la teneur suit :

Chapitre I

DISPOSITIONS GENERALES

Objet

Article 1. La présente charte vise à mettre en place les règles d'utilisation du système d'information de l'université de Guelma et rappeler les responsabilités des utilisateurs ainsi que prévenir et lutter contre les infractions liées aux technologies de l'information et de la communication, dans cet établissement.

Terminologie

Article 2. Au sens de la présente charte, on entend par :

a - Système d'Information : ensemble des moyens techniques et humains, permet de stocker, de traiter ou de transmettre l'information.

b -Système informatique : tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données.

c -Données informatiques : toute représentation de faits, d'informations ou de concepts sous une forme qui seprête à un traitement informatique y compris unprogramme de nature à faire en sorte qu'un systèmeinformatique exécute une fonction.

d -Communications électroniques : toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de renseignements de toutenature, par tout moyen électronique.
e -Administrateur : toute personne possédant une compétence reconnue pour gérer tout ou partie des systèmes d'information ou de télécommunication.

f -Utilisateur : toute personne ayant accès ou utilisant les ressources informatiques et services Internet.

g -Infractions liées aux technologies de l'information et de la communication : les infractions portant atteinte aux systèmes de traitement automatisé de données telles que définies par le code pénal ainsi que toute autre infraction commise ou dont la commission est facilitée par un système informatique ou un système de communication électronique.

Engagement de l'université

Article 3. L'université de Guelma met en œuvre toutes les mesures nécessaires pour assurer la sécurité du système d'information et la protection des utilisateurs, elle facilite l'accès des utilisateurs aux ressources du système d'information.
Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'Université est tenue de respecter la vie privée de chacun.

Article 4. Le centre CRSICT assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'Université. Les agents/personnels de ce centre disposent d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Champ d'application

Article 5.Conformément au décret exécutif n° 12-273 du 08 Chaâbane 1433 correspondant au 28 juillet 2012, modifié et complété, le décret exécutif n° 01-273 du 30 Joumada El Thania 1422 correspondant au 18 septembre 2001, portant création de l'université de Guelma, la présente charte s'applique à tout utilisateur voire administrateur du système d'information de l'établissement.

Chapitre II

DISPOSITIONS RELATIVES A LA SECURITE DU SYSTEME D'INFORMATION

Administrateur du Système d'information

Article 6. L'administrateur veille à :
- mettre en place toutes procédures appropriées pour vérifier la bonne application des règles de contrôle d'accès aux systèmes et aux réseaux définies dans la Politique de Sécurité du Système d'Information, en utilisant des outils autorisés.
- respecter les dispositions légales et réglementaires concernant le système d'information, et pour se faire, de se renseigner, si nécessaire, auprès de sa hiérarchie, de la chaine fonctionnelle SSI, ou des services juridiques de l'établissement.

- respecter la confidentialité des informations auxquelles il accède lors de ses tâches d'administration ou lors d'audit de sécurité, quel qu'en soit le support (numérique, écrit, oral...), en particulier : les données à caractère personnel contenues dans le système d'information, les fichiers utilisateurs, les flux sur les réseaux, les courriers électroniques, les mots de passe, les sorties imprimantes, les traces des activités des utilisateurs ;

- informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître les règles de sécurité à respecter, aidé par le responsable fonctionnel ;

- garantir la transparence dans l'emploi d'outils de prise en main à distance ou toute autre intervention sur l'environnement de travail individuel de l'utilisateur (notamment en cas d'utilisation du mot de passe de l'utilisateur) : limitation de telles interventions au strict nécessaire avec accord préalable de l'utilisateur ;

Article 7. Le droit de l'administrateur dans la sécurité du système d'information consiste à :
- être informé par sa hiérarchie des implications légales de son travail, en particulier des risques qu'il court dans le cas où un utilisateur du système dont il a la charge commet une action répréhensible ;

- accéder, sur les systèmes qu'il administre, à tout type d'informations, uniquement à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations, en s'efforçant - tant que la situation ne l'exige pas - de ne pas les altérer ;

- établir des procédures de surveillance de toutes les tâches exécutées sur la machine, afin de déceler les violations ou les tentatives de violation de la présente charte et de la charte d'usage du système d'information, sous l'autorité de son responsable fonctionnel et en relation avec le correspondant sécurité informatique ;

Article 8. L'administrateur ne doit pas intervenir sur le matériel qui n'appartient pas à l'établissement, sauf à l'isoler du système d'information et du réseau de l'établissement en cas de non-respect des consignes.

Utilisateur du Système d'information

Article 9. Tout utilisateur du système d'information de l'université doit être référencé dans les bases de données et avoir obtenu un code d'accès « authentifiant et mot de passe », qui lui sont personnels et confidentiels. L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité permettant de protéger les données et les outils auxquels il a accès de toute utilisation malveillante ou abusive.

Article 10. Durant l'usage du Système d'information de l'université, l'utilisateur est censé de :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information et aux communications entre tiers pour lesquelles il n'a pas reçu d'habilitation explicite ;

- ne pas utiliser les services qui lui sont offerts pour proposer ou rendre accessibles à des tiers des données et informations confidentielles ou contraires à la législation en vigueur ;

- ne pas installer, télécharger ou utiliser sur le matériel connecté au réseau de l'Université, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de sa hiérarchie ;

- se conformer aux dispositifs mis en place par l'institution pour lutter contre les virus et les attaques par programmes informatiques ;

- ne pas quitter son poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles.

Article 11. L'utilisateur s'engage à ne pas apporter volontairement des perturbations au bon fonctionnement des systèmes informatiques et des réseaux que ce soit par des manipulations anormales du matériel.

CHAPITRE III
DISPOSITION FINALES

Article 12. Les fautes graves seront sanctionnées administrativement dans le cadre des peines prévues par les procédures disciplinaires comme prévu dans le statut général de la fonction publique.

Article 13. Le directeur de l'université et le Chef du Centre CRSICT, ou leurs représentants, se réservent le droit d'engager des poursuites au niveau pénal indépendamment des sanctions administratives mises en œuvre, selon la réglementation en vigueur.

Article 14. En cas de nécessité, le recteur de l'université peut procéder à modifier, ou abroger les clauses de la présente charte sans porter atteinte au bon fonctionnement de la sécurité du SI

Article 15. La présente charte est annexée au règlement intérieur de l'université 8 mai 1945.

En tant qu'utilisateur-administrateur du Système d'Information de l'université, je déclare avoir pris connaissance de la présente charte pour l'usage de ce système et m'engage à la respecter :

Nom et Prénom : ……..….. **Qualité** :…….

E-mail : ……..….**Tél** : …… **Service/Faculté** : ……..

Guelma le : …….

Lu et Approuvé
Signature

Liste des Bibliographies :

[1] http://www.les-infostrateges.com/article/031264/definition-objective-de-l'information

[2] http://www.securitéinf.com

[3] http://www.commentcamarche.net/content/secu/secuintro.php3

[4] Solange Ghernaouti; "Sécurité informatique et réseaux Cours avec plus de 100 exercices corrigés"; 4e edition; Dunod; Paris; 2013

[5] Que sais-je? La Sécurité Informatique; Eric Léopold & Serge Lhoste PUF, Paris; 3éme édition 08/2007

[6] http://medias.dunod.com/document/9782100599127/Feuilletage.pdf

[7]Sécurité informatique – Principes et méthode ; Laurent Bloch & Christophe Wolfhugel ,Eyrolles, Paris 06/2011

[8]CommentCaMarche.net ; Tout sur la Sécurité Informatique ; 2ème édition ;Jean-François Pillou et Jean-Philippe Bay ; Dunod 2009

[9]Thierry BOILEAU, système d'information Par Mise en œuvre de la SSI (Sécurité du Système d'information) de SUSS Micro Optics par l'approche processus ISO/CEI 27001 ; Mémoire présenté en vue d'obtenir le diplôme d'ingénieur cnam spécialité informatique ; 2010

[10]"Etude comparée de référentiels et méthodes utilisées en sécurité informatique",http://www.cases.public.lu/publications/recherche/r2sic/wp11_1.pdf Sabatier, Toulouse

[11] "Rapport de veille sur les standards et méthodes en matière de sécurité informatique", http://www.cases.public.lu/publications/recherche/r2sic/wp11_2.pdf Sabatier, Toulouse

[12] EBIOS, http://www.ssi.gouv.fr/fr/confiance/methodes.html

[13] MEHARI, https://www.clusif.asso.fr/fr/production/mehari/

[14] ITIL, http://www.ogc.gov.uk/index.asp?id=2261

[15] ITIL, http://www.itilfrance.com/

[16] Laborde R., "Un cadre formel pour le raffinement de l'information de gestion de sécurité réseau : Expression et Analyse", Thèse en Informatique, Université Paul.

[17] COBIT, http://www.isaca.org/template.cfm?section=home

[18] CMMI, http://www.sei.cmu.edu/cmmi/

[19] Curtis B., "Describing the Capability Maturity Model", Gartner, 2001

[20] http://www.sei.cmu.edu/arm/SA-CMM.html

[21] http://www.sei.cmu.edu/cmm-p/version2/index.html

[22] http://www.sei.cmu.edu/pub/documents/95.reports/pdf/mm003.95.pdf

[23] BS7799-2, "Information Security Management systems – Specification with guidance for use", BS7799-2: 2002, 2002

[24] Murphy R., "Implementing an ISO 9001:2000-Based Quality Management System: Including Safety and Environmental Considerations", Government Inst, 327 p., ISBN 0865878277, February 2002

[25] ISO 9001, http://www.standardsinfo.net/

[26] Jonquieres M., "Le Manuel du Management Environnemental", Tomes I et II, SAP, Janvier 2001

[27] BS7799-1, "Information technology. Code of practice for information security management", BS7799-1:2000, 2000

[28] http://www.ysosecure.com/ISO-27000/famille-normes-iso-27000.html

[29] http://fr.scribd.com/doc/30445143/Normes-ISO-27000#scribd

[30]http://fr.wikipedia.org/wiki/ISO/CEI_27002

[31] www.datacenter.fr

[32] www.clusif.asso.fr

L'annexe B : fiche-mandat

1. identification du projet

Mandat d'élaboration d'une politique de sécurité de l'information de l'université

Projet no : 01/2015

2. compositions de l'équipe de projet

Mr. Nouar faycel

Mlle. boukhalfa fatima zahra

Mme. hafferssas khadîdja

Mr. Chelaghmia abdelmalek

Mme. Sedraoui soumya

3. échéanciers

L'échéancier de la fin de rédaction des activités du projet est un mois.

4. objectifs du mandat

Objectif de projet est d'élaboré un cadre globale de le politique de sécurité dans l'université ; qui prend en considération les points suivants :

- Organisation de la sécurité
- Sécurité des sites et bâtiments
- Sécurité des locaux
- Réseau étendu intersites
- Réseau local
- Exploitation des réseaux
- Sécurité des systèmes et de leur architecture
- Postes de travail utilisateurs
- Exploitation des télécommunications

La politique qui sera produite devra permettre de :

- se conformer aux lois;
- se conformer aux prescriptions du cadre global d'université;

• assurer la sécurité de l'infrastructure informatique, des actifs informationnels en la continuité de l'activité de l'université en fonction des risques identifiés.

5. les ressources nécessaires à l'élaboration de la politique.

Les ressources humaines nécessaires à la réalisation de la politique sont :

Des ingénieurs en informatique

Des gestionnaires d'informatique

Des spécialistes en réseaux

7. engagements des parties

Date le 01/02/2015

Pour la direction

Pour l'équipe de projet

Annexe B : Questionnaire conforme aux exigences de la Norme 27002

Thème / Questions à poser	R
5- POLITIQUE DE SECURITE	
L'organisation et la gestion de la sécurité sont-elles formalisées dans un document chapeau couvrant l'ensemble du domaine pour l'université ? (PSSI)	**N**
6 -ORGANISATION DE LA SECURITE DE L'INFORMATION	
Quelle a été votre approche du management de la sécurité dans le cadre d'université?	**N**
Avez-vous appliqué une démarche méthodologique d'analyse et de gestion des risques SSI ?	**N**
L'organisation de la sécurité est-elle formalisée dans un document?	**N**
L'université est-elle assurée par un contrat couvrant la perte de personnes clés pour l'activité de l'université ?	**N**
Y'a-t-il une politique de dédoublement u personnel clé de l'université?	**N**
Les rôles et actions des différents acteurs de la SSI ont-ils été définis et ont-ils fait l'objet d'une communication?	**N**
Une politique de confidentialité globale a-t-elle été élaborée ? Si oui, quels sont les sujets abordés (accords de confidentialité)?	**N**
Des révisions périodiques de la mise en œuvre de la gestion de la sécurité sont-elles prévues? Ou bien, des révisions ponctuelles sur événement important sont-elles prévues (évolution fonctionnelle majeure) ?	**N**
7-GESTION DES BIENS	
Existe-t-il un inventaire des biens de l'université?	**N**
Existe-t-il une classification des biens par rapport à leurs critères de sensibilité (en termes de disponibilité, d'intégrité et de confidentialité)?	**N**
8-SECURITE LIEE AUX RESSOURCES HUMAINES	

Des critères spécifiques par rapport à la sensibilité des missions ont-ils été pris en compte lors du recrutement d'une personne pour l'université? Sont-ils spécifiés dans les fiches de postes?	**O**
Le personnel temporaire a-t-il des droits différents des droits des autres utilisateurs?	**N**
Le contrat employeur employé tient il compte des responsabilités de l'employé vis-à-vis de la sécurité de l'organisme ?	**O**
L'organisme s'accorde-t-il les moyens de vérifier l'authenticité et la véracité des diplômes et documents fournis par les potentiels futurs employés ?	**O**
Le responsable /personnel de sécurité est-il formé aux nouvelles technologies ?	**N**
Y a-t-il une procédure d'apprentissage des accidents et des failles de sécurité ?	**N**
A-t-on organisé régulièrement des tests pour vérifier le degré d'assimilation du personnel de la politique de sécurité ainsi que sa culture en informatique.	**N**
Avez-vous formalisé des procédures de retrait des droits d'accès des utilisateurs ainsi que des sous-traitants? (Ces procédures doivent être applicables aux sous-traitants s'ils gèrent les droits d'accès).	**N**
9 SECURITE PHYSIQUE ET ENVIRONNEMENTALE	
La situation géographique de l'organisme tient elle compte des risques naturels?	**N**
Est-ce qu'une analyse de risque a été effectuée pour évaluer la sécurité physique de l'université ?	**N**
Contrôles des portes d'entrée	**N**
Clôtures hautes	**N**
Attribution des badges	**N**
Contrôle à la sortie	**N**
Caméra de surveillance	**N**
Limitation d'accès	**N**
Est-ce que des mesures de sécurité particulière ont été instaurées pour le centre informatique ? (si oui commenter...)	**N**
Y a-t-il une réglementation spéciale contre le fait de fumer, boire, et manger dans les locaux informatiques ?	**N**
Existe-il une protection de câblage informatique et de télécommunication à	**N**

l'égard des risques électrique ? (variation de tension…)	
Les équipements acquis suivent ils une politique de maintenance ?	**N**
Existe-t-il un système de protection contre les coupures et les micros coupures ?	**N**
Existe-t-il un système de climatisation conforme aux recommandations du constructeur ?	**N**
Existe-t-il un groupe électrogène pour les coupures de longue durée ?	**O**
Y a-t-il une procédure de crise en cas de long arrêt ? (favoriser quelques machines sur d'autres…)	**N**
Existence d'un système de détection automatique d'incendie pour l'ensemble de bâtiment	**N**
Existence d'un système d'extinction automatique pour les salles d'ordinateur	**N**
Existence d'extincteurs mobiles	**N**
Existence des meubles réfractaires pour le stockage des documents et des supports informatique vitaux	**N**
A-t-on prévu des systèmes d'évacuation en cas d'incendie ?	**N**
Est-ce que vous êtes assuré que l'eau ne peut envahir les locaux ?	**N**
Est-ce qu'un système de détection d'eau est instauré ?	**N**
Est-ce qu'un système d'évacuation d'eau est instauré ?	**N**
Existe-t-il une documentation liée à la sécurité physique et environnementale ?	**N**
Les matériels sensibles de la plateforme de l'université ont-ils été stockés en fonctions des risques potentiels de menaces extérieures et environnementales (vandalisme au rez de chaussée, crue centennale, etc.)	**N**
Le niveau de disponibilité du système demande-t-il à bénéficier d'un secours électrique? Si oui, comment est-il mis en place?	**N**
Avez-vous pris en compte une gestion de la maintenance pour les matériels de l'université?	**O**
Existe-t-il une procédure de gestion des supports d'informations? Si oui, intègre-t-elle la mise au rebut des supports de stockage (avec procédure d'effacement définitif des données sensibles)?	**N**
10-GESTION DE L'EXPLOITATION ET DES TELECOMMUNICATIONS	

Avez-vous formalisé les procédures d'exploitation de la plate-forme?	**N**
Lors de la réception des matériels et logiciels, des tests sont-ils effectués, notamment des tests spécifiques de sécurité ?	**N**
Toute modification de configuration ou de version fait-elle l'objet d'un plan de conduite de changement appliqué au système?	**N**
Existe-t-il au sein de l'université des mesures de détection, de prévention et de récupération afin de se protéger des codes malveillants?	**N**
Les données sont-elles sauvegardées de manière à garantir leur niveau de confidentialité ? Les données sauvegardées et les supports de sauvegarde bénéficient-ils des mêmes moyens de protection que les données courantes (en intégrité et confidentialité particulièrement) ?	**O**
A-t-on établi un plan de sauvegarde, couvrant l'ensemble des configurations du réseau local, définissant les objets à sauvegarder et la fréquence des sauvegardes ?	**N**
Un niveau de disponibilité des moyens de télécommunication a-t-il été déterminé au sein de l'université ?	**N**
A-t-on vérifié, par une analyse de la charge moyenne et crête de chaque segment de réseau, la compatibilité du réseau et de ses équipements avec cette charge et cette vérification est-elle régulièrement réactualisée ?	**N**
Tous les équipements du réseau local sont-ils couverts par un contrat de maintenance ?	**O**
A-t-on établi une liste des incidents pouvant affecter le bon fonctionnement du réseau local et analysé la criticité de chacun d'eux ?	**N**
Les moyens d'intervention sur le réseau local (tant de diagnostic que de reconfiguration) couvrent-ils de manière satisfaisante tous les cas de figures analysés et permettent-ils de mettre en œuvre les solutions décidées dans les délais spécifiés ?	**N**
Des exigences de sécurité ont-elles été définies pour la gestion des supports amovibles (comment réagir en cas de perte, de vol, etc.)? Si oui, ont-elles fait l'objet d'une communication?	**N**

Existe-t-il des échanges avec l'extérieur de l'information de l'université ? Si oui, sont-ils protégés et comment?	**N**
Les supports en transit contenant des données sont-ils protégés?	**N**
Un service de messagerie est-il utilisé dans l'université ?	**O**
La confidentialité des mails stockés sur les serveurs de messagerie est-elle garantie, comment ?	**N**
Une politique de traçabilité a-t-elle été élaborée au sein de l'université? Si oui, fait-elle une différence entre les traces techniques et les traces métier?	**N**
Quelles sont les mesures de protection mises en place pour protéger les traces en intégrité?	**N**
Quelles sont les mesures de protection mises en place pour protéger les traces en confidentialité?	**N**
Quelle est la durée prévue pour la conservation des traces?	**N**
Quels sont les moyens mis en place afin de s'assurer du non répudiation d'une action?	**O**
Existe-t-il des outils de centralisation et de journalisation des fichiers de journalisation?	**N**
Si oui, existe-t-il un outil d'analyse de ces fichiers de journalisation?	**N**
Une étude a-t-elle été menée afin de déterminer quels fichiers de journalisation sont analysés?	**N**
Y a-t-il des mesures mises en place pour assurer l'intégrité de ces logs?	**N**
Toutes les activités des exploitants du système sont-elles tracées?	**N**
11-CONTRÔLE D'ACCES	
Avez-vous élaboré une politique de contrôle d'accès?	**N**
Avez-vous mis en place une procédure d'enregistrement d'un nouvel utilisateur?	**N**
Tous les nouveaux utilisateurs sont-ils créés avec un profil par défaut ?	**N**
Comment sont gérés les profils au sein de l'université?	**N**
Comment les utilisateurs ont-ils créé leurs comptes au sein du système?	**N**
Une procédure d'attribution des mots de passe a-t-elle été envisagée? (transmission par courrier du mot de passe, par SMS, ...	**N**
La politique d'habilitation prend-elle en compte des révisions des comptes?	**N**

(vérifier que des comptes obsolètes ne soient pas conservés)	
Les bonnes pratiques d'utilisation de mots de passe ont-elles fait l'objet d'une sensibilisation des utilisateurs?	**N**
Les utilisateurs ont-ils été sensibilisés sur la protection des matériel sous leur responsabilité ? (poste de travail, protection de la carte CPS, ne pas donner le code PIN, ...)	**N**
Existe-t-il au sein de l'université des connexions depuis l'extérieur ?	**O**
Le réseau sur lequel est implantée la plateforme de l'université bénéficient-ils de protection particulière? Si oui, de quelles natures sont ces protections?	**O**
Y a-t-il un pare-feu entre le réseau interne et le réseau de la plateforme?	**N**
Les accès au SI sont-ils soumis à des procédures sécurisées? Les exploitants sont-ils authentifiés par des mécanismes d'authentification forte ?	**N**
Quels sont les moyens mis en œuvre pour gérer les autorisations d'accès au système ?	**N**
12-ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION	
Si des éléments sont rapatriés depuis l'extérieur, quelles sont les mesures permettant de garantir l'authenticité et de l'intégrité des informations?	**O**
Quelles mesures permettraient à un utilisateur de vérifier l'authenticité et l'intégrité des informations mises à disposition?	**O**
Avez-vous mené une réflexion sur les moyens cryptographiques à mettre en œuvre? Existe-il une politique de gestion de clés (responsabilités, procédures)?	**N**
Lorsque des modifications de code ou de configuration doivent avoir lieu, des procédures formelles sont-elles appliquées afin d'en contrôler le bon déroulement?	**N**
Avez-vous pris en compte les risques de vol / fuite d'information ? Si oui, quels sont les moyens mis en œuvre?	**O**
13-GESTION DES INCIDENTS LIES A LA SECURITE DE	

L'INFORMATION	
Existe-t-il une cellule de veille d'alerte de sécurité? Si oui, à qui le rapport de veille sont-ils destinés?	**N**
En cas d'incident de sécurité, des fiches d'incident sont-elles créées? Si oui, à qui sont destinées ces fiches?	**N**
Est-il prévu que les utilisateurs du système fasse remonter les informations sur les failles de sécurité?	**N**
Avez-vous formalisé une procédure de gestion des incidents? Si oui, a-t-elle fait l'objet d'un plan de sensibilisation auprès des acteurs?	**N**
14-GESTION DU PLAN DE CONTINUITE DE L'ACTIVITE	
La sensibilité de l'université doit-elle prévoir un plan de reprise de service/d'activité? Si oui, un plan ou une procédure de continuité d'activité a-t-il été formalisé?	**N**
15-CONFORMITE	
Quels sont les moyens mis en œuvre pour garantir que les obligations légales sont bien prises en compte au sein de l'université?	**N**
La politique de sécurité précise-t-elle qu'il est strictement interdit de posséder sur son poste tout logiciel non accompagné d'une licence en règle ?	**N**
Un message de mise en garde indiquant un accès à des données sensibles est-il montré à l'écran de l'ordinateur avant de se connecter ? L'utilisateur doit-il accepter cette mise en garde avant de se connecter ?	**N**

Résumé

Suite à l'engagement de l'administration d'université 8 Mai 1945, Guelma à mettre en place une politique de sécurité de son système d'information réparti sur l'ensemble de ses campus, caractérisé par son importance et sa sensibilité dans la gestion de cet établissement, nous avons effectué une opération d'audit à base des chapitres de la norme ISO 27002, d'où il eut la constatation d'une absence totale du concept de sécurité dans le périmètre étudié, sauf quelques initiatives personnelles.

De ces résultats, nous avons présenté des recommandations et proposé des règles à suivre que devront suivre l'utilisateur voire administrateur de ce système, en se basant sur le domaine organisationnel, environnemental, technique et humain.

Une charte d'usage du système d'information de l'université a été proposée, inspirée de la législation algérienne d'un côté, et les règles de la bonne pratique de ces systèmes de l'autre coté .

Mots clés : Politique de Sécurité, Système d'Information, ISO 27002, Audit, Règle, ISMS, Charte.

ملخص

بعد التزام إدارة جامعة 8 ماي 1945، قالمة لتنفيذ سياسة أمنية لنظم المعلومات الموزعة عبر كافة فروعها، المتميزة بأهميتها وحساسيتها في إدارة هذه المنظمة ، أجرينا عملية التدقيق على أساس فصول معيار ايزو 27002 العالمية، حيث لاحظنا انعدام تام للسياسة الأمنية لنظام معلومات الجامعة، باستثناء بعض المبادرات الشخصية.

من هذه النتائج، اقترحنا مجموعة من التوصيات والقواعد الواجب اتباعها من قبل المستخدم أو مدير النظام، على أساس التنظيمية والبيئية والتقنية والموارد البشرية.

اقترحنا ميثاق استخدام نظام المعلومات في الجامعة، مستوحاة من القانون الجزائري من جانب ، وقواعد الممارسة الجيدة لهذه الأنظمة من الجانب الآخر.

الكلمات المفتاحية: سياسة الأمن ,نظام المعلومات ، ايزو 27002، التدقيق، القاعدة، نظام إدارة أمن المعلومات ، الميثاق

Abstract

Following the commitment of the university administration May 8, 1945, Guelma to implement a security policy for its information systems distributed across all of its campuses, characterized by its importance and sensitivity in managing at this, we conducted an audit operation based chapters of ISO 27002, where it was the finding of a total lack of the safety concept in the area studied, except some personal initiatives.

From these results, we have made recommendations and proposed rules to follow to be followed by the user or administrator of the system, based on organizational, environmental, technical and human.

A usual charter of the university's information system was proposed, inspired by the Algerian law on one side, and the rules of good practice of these systems on the other side

Keywords: Security Policy, Information System, ISO 27002, Audit, Rule, ISMS, Charter.