

الجمهورية الجزائرية الديمقراطية الشعبية  
République Algérienne Démocratique et Populaire  
وزارة التعليم العالي و البحث العلمي  
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique  
مركز البحث في الاعلام العلمي و التقني  
Centre de Recherche sur l'Information Scientifique et Technique



## Post-Graduation Spécialisée en Sécurité Informatique

Promotion 2015

# Projet Fin d'Etude

---

### Thème

Mise en œuvre d'un système de management  
de la sécurité de l'information SMSI au sein  
d'Algérie TELECOM

---

**Encadré par :**

Mme. BENMEZIANE Souad

**Réalisé par :**

M. ZOUGAR Abdellah

## تشكرات REMERCIEMENTS

الحمد لله, والصلاة و السلام على رسول الله, أما بعد :

أعبر عن شكري و امتناني إلى أعضاء إدارة قسم التكوين, من موظفين و أساتذة, لمركز البحث في الإعلام العلمي و التقني, على الجهودات المبذولة من أجل نجاح هذا التكوين .

كما أتقدم بخالص الشكر والتقدير إلى المشرفة على هذا العمل, السيدة بن مزيان سعاد, أستاذة مكلفة بالبحث في مركز البحث في الإعلام العلمي والتقني, على وقتها وعلى المساعدات والنصائح المقدمة من طرفها.

كذلك, أشكر رئيس قسمة أنظمة المعلومات و الفريق العامل فيها, على التسهيلات و المساعدات المقدمة من طرفهم.

أشكر كذلك, أعضاء هيئة المحلفين على قبولهم التقييم على هذا العمل.

و في الأخير, أشكر كل من ساهم في تحقيق هذا العمل, سواء من قريب أو من بعيد.

J'exprime toute ma reconnaissance et gratitude à l'administration, et à l'ensemble du corps enseignant de département Formation, de Centre de Recherche sur l'Information Scientifique et Technique « CERIST », pour leurs efforts à nous garantir la continuité et l'aboutissement de ce programme de PGS Sécurité.

J'adresse mes vifs remerciements à mon encadreur, Mme BENMEZIANE Souad, enseignante Chargée de recherche au ce centre, pour son entière disponibilité, son aide et ses conseils.

Je remercie également le chef, et l'équipe de la DSI d'Algérie Télécom pour leur aide.

Merci également aux membres du jury qui ont accepté d'évaluer mon travail.

Enfin, je tiens à remercier tous ceux qui, de près ou de loin, ont contribué à l'aboutissement de ce travail.

## Résumé du travail :

Initialement, notre principale motivation était liée à la volonté de se démarquer dans le domaine de la protection des systèmes d'informations par la mise en place d'un premier Système de Management de la Sécurité de l'Information « SMSI » au sein d'Algérie Télécom.

Aujourd'hui, les bénéfices ne se mesurent pas seulement en termes d'image mais également sur le fonctionnement en interne.

En effet, la mise en œuvre du SMSI a été l'occasion de mettre en avant l'importance de la sécurité du SI, de la faire reconnaître dans les différents services et de donner aux actions un rythme clair et partagé.

Les exigences pour la mise en place du SMSI sont décrites par la norme ISO/CEI 27001.

Cette norme s'adapte à tout type d'entreprise, quel que soit leur secteur d'activité, sa structure, sa taille et la complexité de son système d'information.

L'application de cette norme passe par une démarche qualitative classique : la roue de Deming (Planifier, Développer, Contrôler, Agir) qui permet de prendre en compte des dysfonctionnements le plus en amont possible et d'amener une amélioration continue du système.

Dans ce travail, on a étudié un cas d'un plan de continuité d'activité du système de messagerie électronique existant, et l'étude des autres cas sera dans le même principe, puis on a proposé un plan d'action et suivi de la réalisation des mesures de sécurité.

A la fin de ce travail, on a réalisé une application support qui facilite la gestion et le contrôle d'application de la politique de sécurité (tel que : A.7 Gestion des actifs et A.11 Contrôle d'accès...etc.).

Cette application permet la bonne maîtrise des actifs, des responsabilités ainsi les accès au système d'information d'Algérie Télécom, elle aide aussi sur la prise des décisions à travers des rapports détaillés sur les actifs et leurs responsables, les accès et les demandes d'accès...etc. , ainsi que le contrôle de l'activité du réseau et la maîtrise des accès.

**Mots clés :** Sécurité de l'information, SMSI, ISO/CEI2700x, PDCA, Actif, contrôle d'accès.

## Table des matières

Introduction Générale .....	09
<b>Chapitre 01 : Un état de l'art des SMSI</b>	
1- Introduction.....	11
2- Définitions.....	11
SMSI (Système de Management de la Sécurité de l'Information).....	11
Comment mettre en place un SMSI ?.....	12
Qu'est-ce qu'une norme ?.....	13
Critères de choix d'une norme.....	13
Normes et standards relatives à la sécurité.....	13
Les normes de la famille ISO/CEI 2700x.....	13
Roue de Deming.....	15
3- La norme ISO/CEI 27001 .....	16
<b>3.1- Phase « PLAN » du PDCA.....</b>	<b>17</b>
3.1.1-Politique et périmètre du SMSI.....	17
3.1.2-Appréciation des risques.....	18
3.1.3-Traitement des risques.....	24
3.1.4-Sélection des mesures de sécurité .....	25
<b>3.2- Phase « DO » du PDCA.....</b>	<b>25</b>
3.2.1-Plan de traitement.....	25
3.2.2-Choix des indicateurs.....	26
3.2.3-Formation et sensibilisation des collaborateurs.....	26
3.2.4-Maintenance du SMSI.....	26
<b>3.3- Phase « CHECK » du PDCA.....</b>	<b>26</b>
3.3.1-Les audits internes.....	26
3.3.2-Les contrôles internes.....	27
3.3.3-Revues de direction.....	27
<b>3.4- Phase « ACT » du PDCA.....</b>	<b>27</b>
3.4.1-Actions correctives.....	27
3.4.2-Actions préventives.....	27
3.4.3-Actions d'améliorations.....	27
4- Conclusion.....	28
<b>Chapitre 02 : Proposition d'une approche Mise en œuvre de la norme ISO / CEI 27001</b>	
1- Introduction.....	29
2- Gestion des risques.....	30
L'objectif de l'étude.....	30
Contexte général de l'étude.....	30
Sujet de l'étude.....	31
2.1- Présentation des méthodes de gestion des risques utilisés.....	32
La méthode INCAS – MESSIE.....	32
La méthode EBIOS.....	34
2.2- Analyse de la sécurité du PCA messagerie électronique.....	34
Contexte.....	34
Objectif.....	34
Description du PCA existant.....	35

Analyse INCAS-MESSIE.....	36
Synthèse de la méthode INCAS-MESSIE.....	51
Analyse EBIOS.....	54
Un plan d'action sur 3 ans .....	54
Synthèse de l'analyse EBIOS.....	64
2.3- Résumé de la partie gestion des risques.....	66
3- Conclusion.....	67

### **Chapitre 03 : Développer une application support pour la politique de contrôle d'accès**

1- Introduction.....	68
2- Définitions.....	68
2.1 contrôle d'accès.....	68
2.2 Droit d'accès.....	68
2.3 Infrastructure Clé Publique (PKI).....	69
2.3.1 Mise en place d'un pilote PKI par la DSI.....	69
2.3.2 Application de la PKI sur les applications du système d'information de l'entreprise...69	69
2.4 Schéma synoptique du réseau d'Algérie Télécom.....	70
3. Politique de contrôle d'accès.....	70
3.1 Exigences métier relatives au contrôle d'accès.....	70
3.1.1 Politique de contrôle d'accès.....	70
3.2 Gestion de l'accès utilisateur.....	71
3.2.1 Enregistrement des utilisateurs.....	71
3.2.2 Gestion des privilèges.....	71
3.2.3 Gestion du mot de passe utilisateur.....	71
3.2.4 Réexamen des droits d'accès utilisateurs.....	71
3.3 Responsabilités utilisateurs.....	71
3.3.1 Utilisation du mot de passe.....	71
3.3.2 Matériel utilisateur laissé sans surveillance.....	71
3.3.3 Politique du bureau propre.....	71
3.4 Contrôle d'accès au réseau.....	72
3.4.1 Politique relative à l'utilisation des services réseau.....	72
3.4.2 Authentification de l'utilisateur pour les connexions externes.....	72
3.4.3 Identification des matériels en réseau.....	72
3.4.4 Protection des ports de diagnostic et de configuration à distance.....	72
3.4.5 Cloisonnement des réseaux.....	72
3.4.6 Mesure relative à la connexion réseau.....	72
3.4.7 Contrôle du routage réseau.....	72
3.5 Contrôle d'accès au système d'exploitation.....	73
3.5.1 Ouverture de session sécurisée.....	73
3.5.2 Identification et authentification de l'utilisateur.....	78
3.5.3 Système de gestion des mots de passe.....	73
3.5.4 Emploi des utilitaires systèmes.....	73
3.5.5 Déconnexion automatique des sessions inactives.....	73
3.5.6 Limitation du temps de connexion.....	73
3.6 Contrôle d'accès aux applications et à l'information.....	73
3.6.1 Restriction d'accès à l'information.....	73
3.6.2 Isolement des systèmes sensibles.....	73
3.7 Informatique mobile et télétravail.....	74
3.7.1 Informatique mobile et télécommunications.....	74
3.7.2 Télétravail.....	74

4. Application Support pour la Politique de Contrôle d'Accès.....	74
4.1 Etude de l'existant .....	74
Procédure de création d'un accès.....	74
Les inconvénients.....	74
4.2 ETUDE CONCEPTUELLE.....	75
4.2.1-Le fonctionnement du système.....	75
4.2.2-Les différentes fonctions de la solution proposée.....	77
Fonctionnalités clés du système de Gestion des Actifs.....	77
Les forces du système de gestion des actifs.....	77
Fonctionnalités clés du système de Gestion des Accès.....	77
Les forces du système de Gestion des Accès.....	77
4.2.3-Présentation générale d'UML.....	77
UML en bref.....	77
Les diagrammes UML.....	78
4.3 Conception du système.....	79
4.3.1. Aspect fonctionnel du système.....	79
Identification des acteurs.....	79
Identification des messages.....	79
Identification des cas d'utilisation.....	80
4.3.2. Aspect dynamique du système.....	81
La modélisation dynamique.....	81
Diagrammes de séquence.....	82
Représentation des diagrammes de séquence.....	82
4.3.3. Aspect statique du système.....	84
Diagramme de classe.....	84
Description détaillée des classes.....	85
Passage vers le modèle relationnel.....	86
Le modèle relationnel .....	86
4.3.4. Conclusion.....	86
4.4 REALISATION.....	87
4.4.1. Introduction.....	87
4.4.2 Architecture de l'application.....	87
4.4.3 Présentation de l'application.....	88
4.4.4. Fonctionnement de l'application.....	88
Fenêtre d'authentification.....	88
Espace Super Administrateur.....	89
Espace Administrateur Actifs.....	89
Espace Administrateur Services.....	90
Tableau de bord « Rapports ».....	90
5. Conclusion.....	91
Conclusion Générale.....	92
Références.....	93
Acronymes.....	94

**Annexe**

Objectifs de sécurité et mesures de sécurité.....	95
A.5 Politique de sécurité.....	95
A.6 Organisation de la sécurité de l'information.....	95
A.7 Gestion des actifs.....	96
A.8 Sécurité liée aux ressources humaines.....	96
A.9 Sécurité physique et environnementale.....	97
A.10 Gestion de l'exploitation et des télécommunications.....	98
A.11 Contrôle d'accès.....	101
A.12 Acquisition, développement et maintenance des systèmes d'information.....	102
A.13 Gestion des incidents liés à la sécurité de l'information.....	104
A.14 Gestion de la continuité de l'activité.....	104
A.15 Conformité.....	104

**Proposition d'un modèle de politique de sécurité « PSSI »**

1- Objet de la politique.....	106
2- Références légales et normatives.....	106
3- Champ d'application de la politique.....	107
4- Les objectifs visés.....	107
5- Classification de l'information.....	107
6- Sécurité des installations informatiques.....	108
7- Sécurité des postes de travail.....	108
8- Sécurité des réseaux.....	108
9- Contrôle d'accès.....	109
10- Sécurité des tiers.....	110
11- Protection des données.....	110
12- Sécurité des Développements et Applications.....	110
13- Acquisition et entretien de matériels et de logiciels.....	110
14- Analyse proactive des menaces technologiques.....	111
15- Utilisation du courrier électronique et d'internet.....	111
16- Gestion de la continuité de l'activité.....	111
17- Gestion d'incidents .....	111
18- Formation et sensibilisation.....	111
19- Sanctions.....	111
20- Responsabilités.....	111
21- Examen.....	111

**Proposition d'un modèle de Charte informatique**

1- Portée.....	112
2- Autorisation d'accès aux ressources informatiques.....	112
3- Respect de la confidentialité des informations .....	112
4- Logiciel.....	112
5- Services Internet.....	113
6- Messagerie électronique.....	113
7- Règles générales de sécurité.....	113

## Liste des figures

### Chapitre 1

Figure 1.1 Normes de la famille ISO/CEI 2700x.....	14
Figure 1.2 : Le modèle PDCA.....	15
Figure 1.3: Structure de l'ISO/CEI 27001.....	16
Figure 1.4 : Etapes de la phase Plan du PDCA.....	17
Figure 1.5 : Processus d'appréciation des risqué.....	18
Figure 1.6 : Modules d'EBIOS.....	20
Figure 1.7 : Utilisation des modules de MEHARI.....	22
Figure 1.8 : Phases de la méthode OCTAVE.....	23

### Chapitre 2

Figure 2.1 : L'échelle de risque.....	33
Figure 2.2 : Processus rétablissement du courant électrique.....	36
Figure 2.3 : Processus Rétablissement du Réseau.....	37
Figure 2.4 : Processus Rétablissement de la disponibilité du système d'exploitation.....	38
Figure 2.5 : Processus Rétablissement de la disponibilité du service de messagerie électronique.....	39
Figure 2.6 : Processus Migration du système de messagerie électronique.....	40
Figure 2.7 : Processus Maintenance du système de messagerie électronique.....	41
Figure 2.8 : Processus Recouvrement après désastre.....	42
Figure 2.9 : Processus Rétablissement du courant électrique©.....	47
Figure 2.10 : Processus Rétablissement du réseau©.....	48
Figure 2.11 : Processus de la disponibilité du système d'exploitation©.....	49
Figure 2.12 : Processus Rétablissement de la disponibilité du service de messagerie électronique©.....	50
Figure 2.13 : Processus Migration du système de messagerie électronique©.....	51
Figure 2.14 : Processus Maintenance du système de messagerie électronique©.....	52
Figure 2.15 : Processus Recouvrement après désastre©.....	53

### Chapitre 3

Figure 3.1: Schéma synoptique du réseau d'Algérie Télécom .....	70
Figure 3.2: Fonctionnement global de la solution.....	76
Figure 3.3 : Les trois aspects disposés par UML .....	78
Figure 3.4 : Le diagramme de cas d'utilisation .....	81
Figure 3.5 : Le diagramme de séquences « Authentification » .....	82
Figure 3.6 : Le diagramme de séquences « Création d'un nouvel Actif ».....	83
Figure 3.7 : Le diagramme de classe.....	84
Figure 3.8 : Architecture de l'application.....	87
Figure 3.9 : Fenêtre d'authentification.....	88
Figure 3.10 : Espace Super Administrateur.....	89
Figure 3.11 : Espace Administrateur actifs.....	89
Figure 3.12 : Espace Administrateur services.....	90

## Liste des tableaux

### Chapitre 1

Tableau 1.1 : Normes ISO/CEI 270xx en préparation.....	14
--	----

### Chapitre 2

Tableau 2.1 : L'échelle de risque.....	33
Tableau 2.2- Rétablissement du courant électrique.....	43
Tableau 2.3- Rétablissement du réseau.....	44
Tableau 2.4- Rétablissement de la disponibilité du système d'exploitation.....	45
Tableau 2.5- Rétablissement de la disponibilité du service de messagerie électronique.....	45
Tableau 2.6- Migration du système de messagerie électronique.....	46
Tableau 2.7- Maintenance du système de messagerie électronique.....	46
Tableau 2.8- Recouvrement après désastre.....	46
Tableau 2.9- besoins de sécurité en termes de disponibilité.....	56
Tableau 2.10- échelle de niveau de gravité.....	56
Tableau 2.11- échelle de niveau de vraisemblance.....	56
Tableau 2.12- Identification des sources de menaces.....	57
Tableau 2.13- Les biens essentiels.....	58
Tableau 2.14- Liens entre biens supports et biens essentiels.....	59
Tableau 2.15- Etude des événements redoutés.....	60
Tableau 2.16- Evaluée des événements redoutés.....	61
Tableau 2.17- Etude des scénarios de menaces.....	62
Tableau 2.18- Evaluation des scénarios de menaces.....	63
Tableau 2.19- Evaluation des risques.....	64
Tableau 2.20- Liste des risques.....	64
Tableau 2.21- Mesures de sécurité.....	65
Tableau 2.22- Echelles de valeur pour le plan d'action.....	65
Tableau 2.23- Plan d'action.....	65

### Chapitre 3

Tableau 3.1 : Description détaillée des classes.....	85
Tableau 3.2 : La méthode de passage vers le model relationnel.....	86