

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Centre de Recherche sur l'Information Scientifique et Technique



Mémoire du projet de fin d'études

**Pour l'obtention du diplôme de Post-graduation spécialisée
en Sécurité Informatique**

Thème :

**Conception d'un
datacenter sécurisé selon
la norme ISO/CEI
27001**

Thème proposé et encadré par :

M. TANJDAOUI Djamel

Etudié par :

Mlle. KALOUNE Yasmina

M. BELGACEM Menad

Devant le jury composé de :

Président du jury : M. NOUALI Omar

Membre du jury : M. BOUDINA AbdelMadjid

Membre du jury : M. HADJAR Samir

 Promotion: 2013 

Résumé

Toute entreprise qui stocke des données informatiques possède un ou plusieurs serveurs. Lorsque le nombre de serveurs est important, il devient utile de les disposer dans un datacenter afin d'optimiser la gestion, l'administration et la sécurisation de ses équipements. Cependant, lors du déploiement de ces datacenters, beaucoup d'entreprises ne tiennent pas compte des différentes normes à respecter. Ces normes contiennent un certain ensemble de paramètres et de recommandations nécessaires pour le bon fonctionnement de ces datacenters.

Mots clés : Datacenter, Sécurité de l'information, Sécurité physique, Sécurité informatique, Sécurité du personnel, Audit, Norme, ISO 27001.



SOMMAIRES



INTRODUCTION GENERALE	01
CHAPITRE I : ETUDE DES DATACENTERS	
I.1. INTRODUCTION	03
I.2. HISTORIQUE	03
I.3. DATACENTER (ETAT DE L'ART)	04
I.3.1. DEFINITION	04
I.3.2. COMPOSANTS	05
I.3.3. CLASSEMENT	07
I.3.4. EVOLUTION	09
I.3.5. PRINCIPAUX ENJEUX	11
I.3.6. RISQUES	12
I.3.7. MENACES	13
I.4. CONCLUSION	13
CHAPITRE II : ETUDE DES DIFFERENTES NORMES POUR DEPLOYER UN DATACENTER	
II.1. INTRODUCTION	14
II.2. PRINCIPE DE SECURITE	14
II.2.1 DEFINITIONS	14
II.2.1.1 SECURITE	14
II.2.1.2 SECURITE d'INFORMATION	14
II.2.1.3 SECURITE INFORMATIQUE	14
II.2.1.4 NIVEAU DE SECURITE	15
II.2.1.5 POLITIQUE DE SECURITE	15
II.2.2. BESOINS DE SECURITE	15
II.2.2.1. PROTECTION DE L'OUTIL DE TRAVAIL	16
II.2.2.2. PROTECTION DES DONNEES	16
II.2.2.3. PROTECTION JURIDIQUE	16
II.2.3. FORME DE SECURITE INFORMATIQUE:	16
II.3. PRINCIPE DE NORME	17
II.3.1 DEFINITIONS	17
II.3.1.1 NORME	17
II.3.1.2 NORME ISO	17
II.3.1.3 NORME ISO 270XX	17
II.3.2 TYPES DE NORME ISO/CEI 270XX	17
II.3.2.1 NORME DE CERTIFICATIONS	17
II.3.2.2 NORME DE RECOMMANDATIONS	18
II.3.2.3 NORMES SECTORIELLES ET TECHNIQUES	18
II.3.3. EVOLUTION DE LA NORME ISO/CEI 270XX	18
II.3.4 STRUCTURE DE LA NORME ISO/CEI 270XX	19
II.3.4.1. ISO/CEI 27001	19
II.3.4.2. ISO/CEI 27002	19
II.3.4.3 ISO/CEI 27003	20
II.3.4.4 ISO/CEI 27004	20
II.3.4.5 ISO/CEI 27005	20

II.3.4.6 ISO/CEI 27006	20
II.3.4.7 ISO/CEI 27007	20
II.3.4.8 ISO/CEI 27008	20
II.3.4.9 NORMES ISO/CEI 270xx EN PREPARATION	21
II.3.5 AUTRE NORMES ET STANDARD	21
II.4 PRINCIPE DE SECURITE NORMATIVE	21
II.4.1 DEFINITIONS	21
II.4.1.1 SYSTEMES DE MANAGEMENT	21
II.4.1.2 SMSI	22
II.4.2 BESOIN D'UN SMSI	22
II.4.3 FONCTIONNEMENT DU SMSI (MODELE DU PDCA)	22
II.4.3.1 PHASE « PLAN » DU PDCA : CONCEVOIR LE SMSI	23
II.4.3.2 PHASE « DO » DU PDCA : IMPLEMENTER ET OPERER LE SMSI	23
II.4.3.3 PHASE« CHECK » DU PDCA : CONTROLER LE SMSI	23
II.4.3.4 PHASE « ACT » DU PDCA : AMELIORER LE SMSI	23
II.4.4 MESURES DE SECURITE SMSI	23
II.5. CONCLUSION	23

CHAPITRE III : CONCEPTION D'UN DATACENTER SELON LES NORMES ETUDIEERS

III.1.INTRODUCTION	24
III.2. PHASE 01 (PRELIMINAIRE)	24
III.2.1. FACTEUR DECLANCHANT	24
III.2.1.1. LIES A LA GESTION DES SYSTEMES DES INFORMATIONS	24
III.2.1.2. INDEPENDANTS LA GESTION DES SYSTEMES DES INFORMATIONS	25
III.2.2. CONSTAT DE L'EXISTANT	25
III.3. PHASE 02 (EXPRESSION DES BESOINS)	25
III.3.1 ANALYSE DES FLUX	25
III.3.1.1 FLUX PHYSIQUES	26
III.3.1.2 FLUX LOGIQUES	26
III.3.1.3 FLUX HUMAINS	26
III.3.2 IDENTIFICATION DES CONTRAINTES	26
III.3.2.1 CONTRAINTES GEOGRAPHIQUES	26
III.3.2.2. CONTRAINTES TECHNIQUES	26
III.3.2.3. CONTRAINTES LOGISTIQUES	26
III.3.2.4. CONTRAINTES ORGANISATIONNELLES	27
III.3.2.5. CONTRAINTES HUMAINES	27
III.3.2.6. CONTRAINTES REGLEMENTAIRES	27
III.4 .PHASE 03 (CONCEPTION)	27
III.4.1 COUCHE PHYSIQUE	27
III.4.1.1 IMPLANTATION DES LOCAUX	28
III.4.1.2 AMENAGEMENTS INTERIEURS	31
III.4.2 COUCHE IT	37
III.4.2.1 ATTAQUES ET PARADES	37
III.4.3 COUCHE APPLICATIFS	38
III.5. CONCLUSION	39

CHAPITRE IV : AUDITER UN DATACENTER

IV.1. INTRODUCTION	40
IV.2. PRINCIPES DE L'AUDIT	40
IV.2.1 DEFINITIONS	40

IV.2.1.1 AUDIT	40
IV.2.1.2 AUDITEUR	40
IV.2.2 CARACTERISTIQUES DE L'AUDIT	40
IV.2.2.1 INTEGRITE	40
IV.2.2.2 SINCERITE	40
IV.2.2.3 LA CONSCIENCE PROFESSIONNELLE	41
IV.2.2.4 CONFIDENTIALITE	41
IV.2.2.5 INDEPENDANCE	41
IV.2.2.6 APPROCHE FONDEE SUR LES PREUVES	41
IV.2.3. DIFFERENTS TYPES D'AUDIT	41
IV.3. AUDIT	42
IV.3.1. STRUCTURE D'ACCUEIL	42
IV.3.2. DEMARCHE DE L'AUDIT	43
IV.3.2.1. PREPARATION DE L'AUDIT	43
IV.3.2.2. AUDIT ORGANISATIONNEL ET PHYSIQUE	43
IV.3.2.3. AUDIT TECHNIQUE	44
IV.3.2.4. AUDIT INTRUSIF	45
IV.3.3. CONCLUSION DE L'AUDIT	45
IV.3.3.1. CONCLUSION DE L'AUDIT ORGANISATIONNEL ET PHYSIQUE	45
IV.3.3.2. CONCLUSION DE L'AUDIT TECHNIQUE	49
IV.4. CONCLUSION	60
CONCLUSION GENERALE	61
REFERENCES	
ANNEXES	