

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 pour l'obtention du diplôme
de Post Graduation Spécialisée en Sécurité Informatique

Thème

ETUDE COMPARATIVE DES METHODES DE GESTION DES RISQUES MEHARI, EBIOS ET OCTAVE

Elaboré par:

- BENANTAR Khaled
- DEGHBAR Omar

Encadré par :

- Mme. BENMEZIANE Souad

Soutenu devant le jury :

- Dr, ALIANE Hassina, Maître de Recherche CERIST, Présidente.
- Mr, BOUDINA AbdelMadjid, Attaché de Recherche CERIST, Examineur.
- Mr, MEKANNE Salem, Chargé d'étude CERIST, Examineur.

-Année 2012-

Remerciements

En préambule à ce mémoire, nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous a apporté leur aide et qui ont contribué à l'élaboration de ce mémoire ainsi qu'à la réussite de cette formidable année PGS au CERIST.

Nous tenons à remercier sincèrement notre promotrice Madame BENMEZIANE Souad pour la confiance qu'elle nous a témoignée en nous proposant ce sujet, sa disponibilité tout au long du projet, ses encouragements et sa patience. Les discussions scientifiques qu'elle a su générer, ses remarques et ses suggestions nous ont permis de finaliser ce travail.

Nous exprimons toute notre profonde gratitude et nous les remercions pour le personnel du service formation du CERIST.

Nous remercions les membres du jury pour avoir bien voulu juger notre travail.

Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous a toujours soutenu et encouragé au cours de la réalisation de ce mémoire. Merci à tous et à toutes.

Résumé

Sécuriser un système d'information revient à essayer de se protéger contre les risques liés à l'informatique pouvant avoir un impact sur la sécurité de celui-ci, ou des informations qu'il traite.

Afin de sécuriser les Systèmes d'information nous pouvons donc avoir recours à des méthodes des gestions des risques ou d'audit selon les besoins en sécurité engendrés par le Système d'information. En effet, nous nous tournerons vers des méthodes différentes selon le contexte dans lequel nous évoluerons.

Notre objectif est d'étudier les différentes méthodes de gestion des risques existantes (MEHARI, EBIOS et OCTAVE) ainsi que les normes internationales (ISO 27005 : 2008).

L'étude comparative nous a permis de cerner les objectifs de chacune de ces méthodes et les différences qui les caractérisent.

A la fin nous avons réalisé une simulation de la méthode EBIOS sur une plateforme de télé-enseignement au niveau du service de formation du CERIST.

Mot clé : Risque, ISO 27005, MEHARI, EBIOS, OCTAVE

Sommaire

Introduction Générale.....	1
Chapitre 1 : Présentation de la gestion des risques	2
1. Introduction	2
2. Concepts de la gestion des risques	2
2.1. Actifs	3
2.2. Notion de menace	4
2.3. Notion de vulnérabilité	4
2.4. Définition du risque.....	5
3. Options fondamentales de gestion des risques	6
3.1. Gestion directe et individualisée des risques	7
3.2. Gestion globale et indirecte des risques.....	7
4. Le processus de gestion de risque.....	8
4.1. Identification des risques.....	8
4.2. Estimation des risques	9
4.2.1. Estimation des risques pour leur gestion individualisée.....	9
4.2.2. Estimation des enjeux ou des conséquences du risque.....	10
4.2.3. Estimation du niveau de menace	10
4.2.4. Estimation du niveau de vulnérabilité	10
4.3. Evaluation des risques	11
4.4. Traitement des risques	12
5. Conclusion	12
Chapitre 2 : Méthodes d'analyse des risques	13
1. Introduction	13
2. MEHARI	13
2.1. Introduction	13
2.2. Démarche Méhari	14
2.2.1. Phase préparatoire.....	14
2.2.2. Phase opérationnelle d'analyse des risques.....	18
2.2.3. Phase de planification et de traitement des risques.....	21
2.3. Outil.....	23
3. EBIOS	24
3.1. Introduction	24
3.2. Domaine d'application	24
3.3. Démarche EBIOS	25
3.3.1. Module 1 – Étude du contexte	25
3.3.2. Module 2 – Étude des événements redoutés	26
3.3.3. Module 3 – Étude des scénarios de menaces	26
3.3.4. Module 4 – Étude des risques	26
3.3.5. Module 5 – Étude des mesures de sécurité	27
3.4. Outil.....	27
4. OCTAVE	28
4.1. Introduction	28
4.2. Démarche OCTAVE.....	28

Phase 1 : Vue organisationnelle	29
Phase 2 : Vue technique	30
Phase 3 : Développement de la stratégie	30
4.3. OUTIL	30
Chapitre 3 : La comparaison des méthodes	31
1. Introduction	31
2. Objectifs	31
3. Contenu de la norme :	31
3.1. Démarche proposée par l'ISO/CEI 27005	32
3.1.1. Etablissement du contexte :	32
3.1.2. Appréciation des risques :	33
3.1.3. Traitement du risque :	33
3.1.4. Acceptation du risque :	33
3.1.5. Communication du risque :	34
3.1.6. Surveillance et Réexamen du risque :	34
3.2. Outil	34
4. Tableau de comparaison au processus SMSI	35
5. Tableau de comparaison des méthodes :	37
6. Synthèse	39
7. Critères de choix d'une méthode	40
Chapitre 4 : Simulation de la méthode EBIOS	41
1. Introduction	41
2. Présentation du service de la formation continue, de perfectionnement et de recyclage	41
2.1. Responsable de la formation	41
2.2. Section formation continue et de recyclage du personnel	41
2.3. Section séminaires de formation :	42
2.4. Section Formation de la post graduation spécialisées	42
2.5. Section de Téléenseignement	43
3. Présentation du système de télé-enseignement	43
3.1. Architecture globale du système de télé-enseignement	44
3.2. Equipement et logiciels déployés	44
3.3. Application de la méthode EBIOS	45
Module 1 – Étude du contexte	45
Activité 1.1 – Définir le cadre de la gestion des risques	45
Activité 1.3 – Identifier les biens	50
Module 2 – Étude des évènements redoutés	54
Module 3 – Étude des scénarios de menaces	57
Action 3.1.2 Evaluation des scénarios de menaces :	67
Module 4 – Étude des risques	68
Activité 4.1 – Apprécier les risques	68
Action 4.1.1 : Analyser les risques	68
Action 4.1.2 Évaluer les risques	69
Activité 4.2. Identifier les objectifs de sécurité	70
Action 4.2.1. Choisir les options de traitement des risques	70
Module 5 – Étude des mesures de sécurité	70
Conclusion générale	71
Bibliographie :	73