MEHARI-Pro

Vue d'ensemble et principes directeurs

Version 1,3

Novembre 2013

Club de la Sécurité de l'Information du Québec
Téléphone : + 1 (418) 564-9244
Télécopieur : + 1 (418) 614-0842
Courriel : administration@clusiq.org

Remerciements

L'ASIQ[1] tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Sylvain	Bertrand	Hydro Québec
Simon	Borduas	Conseiller en gestion de risque
Dominique	Buc	BUC S.A.
Olivier	Corbier	Docapost Responsable de l'Espace Méthodes du Clusif
Colette	Fournier	Hydro Québec
Martine	Gagné	Conseillère en gestion de risque
Christophe	Jolivet	Pr4gm4
Jean-Philippe	Jouas	Fondateur de la méthode et membre honoraire de l'ASIQ
Chantale	Pineault	AGRM – Protection de l'information
Jean-Louis	Roule	Responsable du Groupe de Travail Documentation de MEHARI, au sein du Clusif
Claude	Taillon	Conseiller en sécurité de l'information

[1] ASIQ : Association de sécurité de l'information du Québec

Sommaire

Introduction

MEHARI-Pro fait partie de l'ensemble des méthodes d'analyse de risques développées à partir du modèle d'analyse de risques créé par Jean-Philippe Jouas et Albert Harari en 1992, modèle utilisé par le CLUSIF, pour MEHARI, depuis 1996.

MEHARI-Pro est une méthode rigoureuse de gestion de risque destinée aux professionnels de la sécurité. Elle vise principalement les petites ou moyennes organisations, privées ou publiques, ou encore les organisations plus importantes qui souhaitent, au moins dans un premier temps, avoir une vision et une analyse globale de leurs risques sans entrer dans le détail de l'infrastructure et du fonctionnement des systèmes d'information et de communication.

MEHARI-Pro est une méthodologie basée sur les mêmes processus d'analyse et d'évaluation des risques que l'ensemble des variantes de MEHARI en utilisant une base de connaissances spécifiques adaptée à la cible visée.

Ses domaines d'application, sont principalement :

- La gestion permanente des risques auxquels l'organisation est confrontée
- L'analyse ponctuelle des risques induits par une nouvelle application, de nouvelles fonctionnalités d'un système d'information ou la mise en place d'un nouveau système d'information;

Le premier objectif de MEHARI-Pro est de fournir une méthode d'analyse et de gestion des risques et, plus particulièrement pour le domaine de la sécurité de l'information, une méthode conforme aux exigences de la norme ISO/IEC 27005:2008, avec l'ensemble des outils et moyens requis pour :

- Identifier de manière précise et exhaustive les situations de risque auxquelles l'organisation doit faire face.
- Permettre une analyse directe et individualisée des situations de risque décrites par des scénarios de risque.
- Proposer des mesures de sécurité permettant de réduire les risques jugés inacceptables et permettre d'en évaluer l'effet sur les niveaux de risques résiduels.

À cet objectif premier s'ajoute l'objectif complémentaire de fournir une gamme d'outils adaptée à la gestion de la sécurité de l'information, et ce, quels que soient les types d'actions envisagés.

Compte-tenu de ces objectifs, MEHARI-Pro propose un ensemble méthodologique cohérent, faisant appel à des bases de connaissances adaptées et capables d'accompagner les responsables de la sécurité dans leurs différentes démarches et actions, incluant des acteurs impliqués dans la gestion des risques.

Principes directeurs

Cette déclinaison de MEHARI, comme toutes les autres, respecte les principes directeurs suivants :

- Identifier les situations de risque par une démarche structurée et arborescente partant des activités de l'organisation et en recherchant les dysfonctionnements possibles et leurs causes.

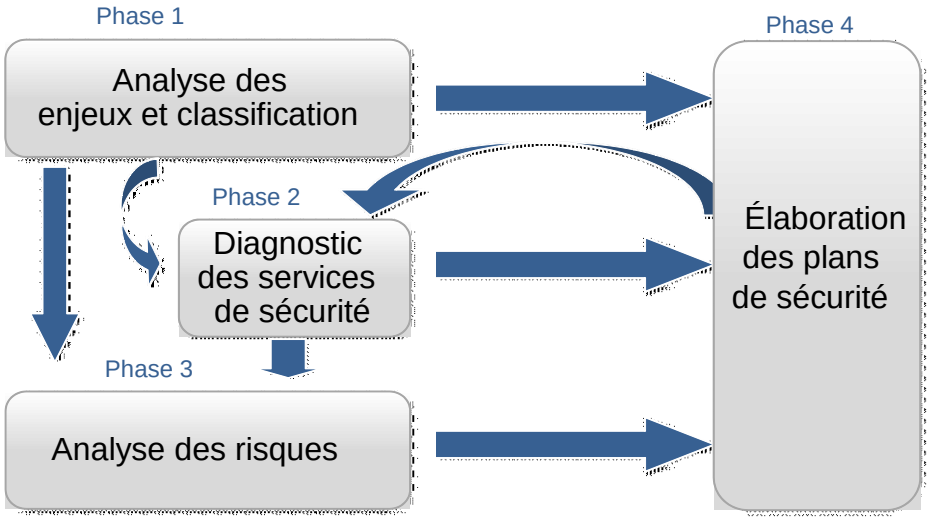
- Évaluer les conséquences d'un risque potentiel à partir d'une classification des actifs, elle-même basée sur les impacts maximum des risques sur les processus d'affaires de l'organisation.
- Évaluer la probabilité de survenance d'un risque à partir de la potentialité initiale d'occurrence de l'événement.
- Tenir compte, dans l'évaluation d'un risque, non seulement des mesures de sécurité existantes mais aussi de leur niveau de qualité et d'efficacité.
- Appuyer l'évaluation de la qualité des mesures de sécurité en place (ou prévues) sur une base de connaissance apportant l'expertise requise.

Vue d'ensemble de MEHARI-Pro

MEHARI-Pro consiste à :

- procéder à l'analyse des enjeux et à la classification des actifs de l'organisation (DIC);
- procéder à un diagnostic de la qualité des services de sécurité en place (vulnérabilité);
- identifier les scénarios de risques plausibles pouvant altérer la qualité (DIC) ou le fonctionnement des actifs impliqués;
- identifier les mesures de sécurité à mettre en place pour réduire la gravité des risques non acceptables et décider des actions à entreprendre sur les autres risques;
- élaborer un plan d'action priorisant les mesures ayant le plus grand effet sur l'atténuation des risques.

Le schéma ci-dessous résume la démarche.



Les forces de l'approche actuelle de MEHARI-Pro :

- Simplicité de l'application de la méthode;
- Rigueur de l'approche méthodologique;

- Richesse et cohérence de sa base de connaissances qui est une extraction de celle de MEHARI-EXPERT;
- Prise en compte des niveaux de qualité des mesures de sécurité pour évaluer les risques résiduels (en effet, l'efficacité des mesures de sécurité pour réduire les risques dépend des mécanismes adoptés et de leur robustesse)
- Prise en compte des niveaux d'efficacité d'une mesure de sécurité pour diminuer les risques (en effet, certaines mesures de sécurité apportent plus de valeur ajoutée);
- Facilité, pour un non-spécialiste, de bien analyser les situations et de proposer des mesures tenant compte de la maturité et de la capacité de l'organisation à mettre en œuvre les solutions proposées;
- Simplicité d'illustration de la progression en matière de gestion de risques de l'organisation.

MEHARI-Pro se caractérise comme suit :

Pour les actifs (voir annexe A1)

- 6 actifs de type « données et informations » soit :
  - ✓ Fichiers informatiques (applicatifs)
  - ✓ Données informatiques isolées qu'elles soient stockées, temporaires ou en transit
  - ✓ Fichiers bureautiques
  - ✓ Courrier électronique
  - ✓ Documents non informatiques, imprimés ou manuscrits
  - ✓ Informations publiées ou services accessibles sur un serveur Internet
- 4 actifs de type « services » soit :
  - ✓ Services informatiques et de télécommunication
  - ✓ Équipements mis à la disposition des utilisateurs (ordinateurs, imprimantes locales, périphériques, interfaces spécifiques, etc.)
  - ✓ Services offerts sur sites Internet
  - ✓ Environnement de travail des utilisateurs

Pour les services de sécurité

- ✓ 43 services de sécurité caractérisés par 377 questions
- ✓ 74 scénarios de risques répartis comme suit :
  - 38 scénarios en disponibilité
  - 15 scénarios en intégrité
  - 21 scénarios en confidentialité

La liste des services de sécurité est donnée à l'annexe A2 alors que les scénarios de risques sont décrits dans le fichier Excel de MEHARI-Pro.

1.1. L'analyse des enjeux

Quelles que soient les orientations ou la politique, en matière de sécurité de l'information, il y a un principe sur lequel tous les gestionnaires s'accordent, c'est celui de la juste proportion entre les moyens investis dans la sécurité et la hauteur des enjeux de cette même sécurité.

L'objectif de l'analyse des enjeux est de répondre à cette double question :

« Que peut-on redouter et, si cela devait arriver, serait-ce grave? (l'organisation serait-elle en mesure d'y faire face?) »

Tout comme pour MEHARI-Expert, MEHARI-Pro intègre un module d'analyse des enjeux, qui aboutit à deux types de résultats :

1. Une échelle de valeurs des dysfonctionnements.

2. Une classification des informations et des actifs du système d'information.

Échelle de valeurs des dysfonctionnements

La recherche des dysfonctionnements généraux dans les processus opérationnels ou des événements que l'on peut redouter est une démarche qui s'exerce à partir des activités de l'organisation. Une telle démarche mène à :

- Une description des types de dysfonctionnements redoutés pouvant affecter la disponibilité, l'intégrité ou la confidentialité.
- Une définition des paramètres qui influencent la gravité de chaque dysfonctionnement.

L'évaluation des seuils d'impact ou de criticité de ces paramètres qui font passer la gravité des dysfonctionnements d'un niveau à un autre, cet ensemble de résultats constitue une échelle de valeurs des dysfonctionnements.

Classification des informations et des actifs

Il est d'usage, dans le domaine de la sécurité de l'information, de parler de la classification des informations et des actifs du système d'information.

Cette classification consiste à définir pour chaque type de processus d'affaires, l'information indispensable (actif primaire) et, pour chaque information, les systèmes d'information les supportant (actif de soutien) et, pour chacun des critères de classification (soit la *Disponibilité*, l'*Intégrité* et la *Confidentialité*), des indicateurs représentatifs de la gravité d'une atteinte à ce critère pour cette information ou cet actif.

La classification des informations et actifs est la traduction, pour les systèmes d'information, de l'échelle de valeurs des dysfonctionnements, définie précédemment, en indicateurs de sensibilité associés aux actifs du système d'information (aussi appelé « Sensibilité DIC »).

Expression des enjeux de la sécurité

L'échelle de valeurs des dysfonctionnements et la classification des actifs sont deux manières distinctes d'exprimer les enjeux de la sécurité.

La première est plus détaillée et fournit plus de renseignements pour des responsables de sécurité alors que la seconde est plus globale et facilite la communication sur le degré de sensibilité DIC des actifs, avec moins de précision.

1.2. Les diagnostics des services de sécurité

MEHARI-Pro intègre des questionnaires de diagnostic extraits de MEHARI-Expert et tient compte de plusieurs mesures de sécurité qui sont inspirées d'ISO 27002[2]. Les questionnaires permettent de mesurer la qualité des services effectivement en place de même que le niveau de qualité des mécanismes et solutions mis en place pour réduire les risques.

1.2.1 Le diagnostic de sécurité, élément clé d'une analyse des risques

Disons simplement, à ce niveau, que le modèle de risque prend en compte des « facteurs de réduction de risque » qui sont concrétisés par l'existence des services de sécurité en place.

Le diagnostic de ces services sera donc, lors de l'analyse des risques, un élément important d'assurance que les services en place remplissent bien leur rôle, ce qui est essentiel pour qu'une analyse de risque soit crédible et fiable.

MEHARI-Pro s'appuie sur une base de diagnostic reconnue d'évaluation de la qualité des mesures de sécurité en place ou planifiées, ce qui en fait une méthode crédible lors de l'évaluation des risques et de la planification des plans d'action.

1.3. L'analyse (ou appréciation) des risques

L'analyse de risques est citée dans beaucoup d'ouvrages sur la sécurité de l'information, et notamment dans les normes ISO/IEC de la série 27000, comme devant être la base de l'expression des besoins de sécurité.

MEHARI propose, depuis plus de 15 ans, une approche structurée du risque[3] qui repose sur quelques éléments simples.

Pour l'essentiel, une situation à risque peut être caractérisée par divers facteurs :

- Des facteurs structurels qui ne dépendent pas des mesures de sécurité, mais du domaine d'affaires de l'entreprise, de son environnement et de son contexte.
- Des facteurs de réduction de risques qui sont, eux, directement fonction des mesures de sécurité mises en place.

Précisons simplement qu'une analyse des enjeux est nécessaire pour déterminer la gravité maximale des conséquences d'une situation à risque, ce qui est typiquement un facteur structurel,

---

[2] Les mesures de sécurité sont groupées par sous-services, qui sont regroupés par services de sécurité puis par domaines de sécurité.

[3] Le détail du modèle de risques est disponible dans le document *« Principes fondamentaux et spécifications fonctionnelles de MEHARI »*.

alors que des diagnostics de sécurité sont nécessaires pour évaluer les facteurs de réduction de risques.

MEHARI-Pro permet d'évaluer ces facteurs et de porter un jugement sur le niveau de risques. MEHARI s'appuie, pour cela, sur des outils (critères d'appréciation, méthodes de calcul, etc.) et des bases de connaissances (en particulier pour les diagnostics de sécurité) qui s'avèrent indispensables en complément du cadre minimum proposé par la norme ISO 27005.

1.3.1 L'analyse systématique des situations de risques

Pour répondre à la question « À quels risques l'organisation est-elle exposée et ces risques sont-ils acceptables? », une méthode structurée consiste à évaluer toutes les situations de risque potentielles, à identifier individuellement les plus critiques, puis à décider des actions à mener afin de les ramener à un niveau acceptable.

MEHARI-Pro permet de réaliser cette analyse et les bases de connaissance ont été développées afin d'atteindre cet objectif. Dans cette utilisation de MEHARI, l'accent est mis sur l'assurance que les situations critiques les plus souvent rencontrées ont été prises en compte et sont bien couvertes par un plan d'action.

Cette méthode s'appuie sur une base de connaissances de situations de risques et sur des mécanismes d'évaluation des facteurs caractérisant chaque risque et permettant d'en apprécier le niveau. La méthode fournit, en outre, des aides pour définir les plans de traitement adaptés.

Actuellement, avec la base de connaissance, le processus d'appréciation des risques est soutenu par un ensemble de fonctions de la base de connaissances (Microsoft Excel) permettant d'intégrer les résultats des divers modules de MEHARI (classification des actifs résultant de l'analyse des enjeux et diagnostics de sécurité des différents services de sécurité). Ces fonctions permettent d'évaluer les niveaux de risques actuels et de proposer des mesures additionnelles pour réduire la gravité des scénarios de risques.

Ultérieurement, il sera possible d'utiliser un outil logiciel offrant une assistance évoluée et permettant de faire des simulations, des visualisations et des optimisations.

1.4. Le plan d'action en sécurité de l'information

À l'issue de la phase d'analyse des risques et des prises de décision concernant le traitement des risques, l'organisation doit statuer sur un certain nombre d'actions à mener qui relève, selon le type de traitement retenu :

- De la mise en place de services de sécurité, avec pour chacun, un objectif de niveau de qualité.
- De mesures structurelles visant à réduire certaines expositions aux risques.
- De mesures organisationnelles visant à éviter certains risques.

Ceci étant dit, il doit être clair que toutes ces actions ne seront sans doute pas menées simultanément ni toutes engagées immédiatement, pour diverses raisons telles que la limitation des ressources budgétaires, l'indisponibilité des ressources humaines, etc.

Dans ces conditions, la phase d'élaboration des plans d'action doit inclure les étapes suivantes :

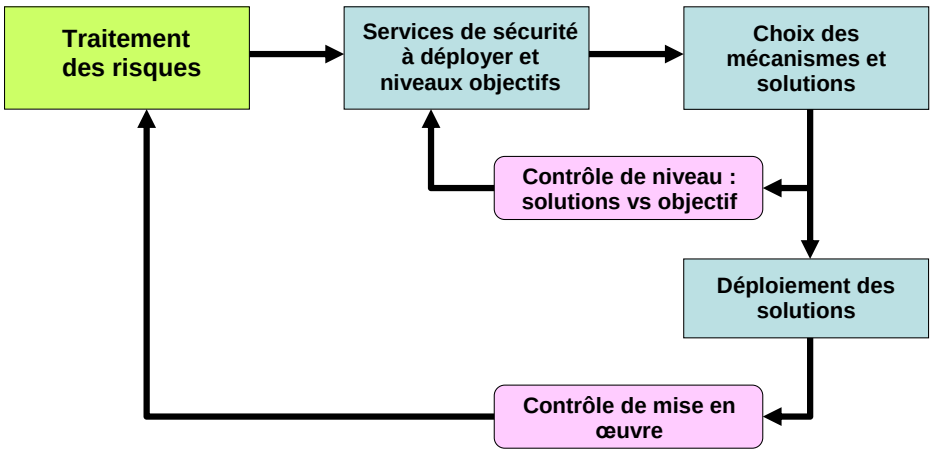
- le choix des objectifs prioritaires, en termes de services de sécurité à mettre en œuvre (ou à améliorer) et l'optimisation de ce choix reposant sur les risques les plus élevés à atténuer et sur la capacité de l'organisation à les mettre en œuvre;
- la transformation des choix de services de sécurité (à implanter ou à améliorer) en plans

d'action concrets;

- le choix des mesures structurelles éventuelles et des mesures d'évitement des risques;
- la validation des décisions précédentes par la haute direction.

1.5. Contrôle et pilotage de la gestion directe des risques

Les contrôles à effectuer pour piloter la gestion directe des risques sont multiples et sont représentés par le schéma suivant :



Le premier niveau de contrôle à effectuer vise à s'assurer que les mécanismes et solutions de sécurité planifiés et décidés correspondent bien au niveau de qualité des services retenus et en phase de traitement des risques.

Le deuxième contrôle est un contrôle de mise en œuvre.

1.5.1 Contrôle du niveau de qualité des services retenus

Ce contrôle cherche à savoir comment le personnel technique en charge de définir les mécanismes et solutions à mettre en œuvre va pouvoir le faire avec une connaissance suffisante de l'impact de leurs décisions sur le niveau de qualité du service qui sera obtenu une fois implanté.

Par ailleurs, un contrôle a posteriori sera nécessaire et ce contrôle devra être effectué par du personnel qui ne sera pas obligatoirement un technicien confirmé et d'expérience.

Cela conduit à la nécessité d'une base d'expertise ou base d'audit des services de sécurité qui permettra des choix appropriés lors de la phase de définition des mécanismes et des solutions à mettre en œuvre, d'une part, et un contrôle a posteriori, d'autre part.

Justification de la nécessité d'une base d'audit des services de sécurité

Dans les principes de MEHARI, et bien entendu dans ses bases de connaissances, la qualité des services de sécurité comprend trois aspects que sont leur efficacité, leur robustesse et leur mise sous contrôle.

Pour pouvoir vérifier chacun de ces aspects, des questions spécifiques devront être posées.

Il est alors nécessaire qu'il y ait une ligne directrice et un répertoire des questions à poser et qu'à ces questions soit associé un système de cotation des réponses pour pouvoir qualifier de manière fiable et reproductive la qualité de chaque service de sécurité.

MEHARI-Pro comprend une base de questionnaires (qui est un extrait adapté de la base de MEHARI-Expert 2010) ainsi qu'un système de pondération décrit dans le « Guide du diagnostic de l'état *des services de sécurité* » et reposant sur les mêmes prémisses.

1.5.2 Contrôle de la mise en œuvre des services de sécurité

Il est bien clair que la mise en œuvre effective des services de sécurité définis précédemment devra être contrôlée.

On sera souvent amené à constater des situations dans lesquelles des services de sécurité ont été partiellement déployés et où leur mise en œuvre n'est pas totalement conforme aux décisions prises au préalable.

Du point de vue de la gestion des risques la conduite à tenir dans de tels cas est explicitée dans la documentation d'accompagnement de la méthode.

1.5.3 Pilotage global associé à la gestion des risques

Le pilotage global de la gestion directe des risques ressemble à tout pilotage de projet et comprend :

- Des indicateurs et un tableau de bord;
- Un système de rapport;
- Un système de revue périodique et de prise de décision relative aux actions correctives nécessaires.

Annexe A1

Typologie d'actifs (T1) de la base de connaissances de MEHARI-Pro

Tableau T1	Actifs de type données															Actifs de type service				
Processus métier, domaine applicatif ou domaine d'activité **Services communs à particulariser**	Fichiers informatiques			Données informatiques isolées, en transit			Fichiers bureautiques			Courrier électronique			Documents non informatiques, imprimés ou manuscrits		Informations ou services offerts sur Internet	Services informatiques et de télécommunication		Equipements mis à la disposition des utilisateurs	Services offerts sur sites Internet	Services généraux environnement de travail
	D	I	C	D	I	C	D	I	C	D	I	C	D	C	I	D	I	D	D	D
Types d'actifs	D01	D01	D01	D02	D02	D02	D03	D03	D03	D04	D04	D04	D05	D05	D06	S01	S01	S02	S03	G01
Processus métiers																				
Domaine 1 :																				
Domaine 2 :																				
Domaine 3 :																				
Domaine 4 :																				
Domaine 5 :																				
Domaine 6 :																				
Domaine 7 :																				
…/…																				
Domaine N																				
Processus transverses																				
Processus 1																				
Administration/ politique d'ensemble																				
Classification pour l'ensemble																				
Classification pour le périmètre choisi																				

La synthèse des classifications (maximum) par colonne est effectuée automatiquement : pour ajouter ou supprimer des domaines utiliser les fonctions " insérer " une ligne ou "supprimer " une ligne.
La classification (maximum de chaque colonne) est reportée dans le tableau d'impact intrinsèque, pour chaque type de données dans la colonne correspondant au critère de classification (D, I ou C)

Annexe A2

Liste des 43 services de sécurité appelés par MEHARI-Pro

(377 questions et descriptions)

SERVICES ET SOUS-SERVICES DE SÉCURITÉ

01 Organisation de la sécurité (01 Org)

A - Rôles et structures de la sécurité

1A01 Organisation et pilotage de la sécurité des systèmes d'information

1A02 Système général de déclaration et de gestion des incidents

1A03 Gestion des prestataires ou fournisseurs de services externes

B - Gestion des ressources humaines et des prestataires

1B01 Prise en compte de la sécurité dans les relations avec le personnel informatique (salariés et prestataires)

02 Sécurité physique (02 Phy)

A - Protection contre les risques environnementaux divers

2A01 Analyse et traitement des risques environnementaux divers

2A02 Continuité de la fourniture d'énergie

2A03 Sécurité des équipements de servitude

B - Contrôle des accès physiques

2B01 Contrôle des accès aux locaux sensibles

2B02 Détection des intrusions dans les locaux sensibles

2B03 Surveillance des locaux sensibles

C - Protection de l'information écrite

2C01 Conservation et protection des documents et supports amovibles importants

2C02 Sécurisation du circuit de création, de diffusion et de destruction des documents

03 Sécurité des systèmes et de leur architecture (03 Sys)

A - Contrôle d'accès aux systèmes, applications et données informatiques

3A01 Contrôle des accès internes aux systèmes, aux applications et données (gestion des droits, authentification et filtrage)

3A02 Contrôle des accès externes au réseau interne

B - Sécurité de l'architecture

3B01 Sûreté de fonctionnement des éléments d'architecture

3B02 Sécurité des serveurs de site Internet

04 Exploitation des systèmes d'information et de communication (04 Exp)

A - Sécurité des procédures d'exploitation des systèmes d'information et de communication

4A01 Contrôle de la mise en production de nouveaux systèmes ou d'évolutions de systèmes existants

4A02 Prise en compte de la confidentialité lors des opérations de maintenance sur les systèmes et les postes utilisateurs

B - Gestion des supports informatiques de données et programmes

4B01 Sécurité physique des supports

C - Continuité de fonctionnement

4C01 Organisation de la maintenance des systèmes (matériel et logiciel)

4C02 Procédures et plans de reprise des applications sur incidents d'exploitation

4C03 Sauvegarde des configurations logicielles (logiciels de base et applicatifs et paramètres de configuration, configurations des postes utilisateurs)

4C04 Sauvegarde des données (des serveurs applicatifs et bureautiques)

4C05 Plans de Reprise d'Activité des services informatiques

4C06 Protection antivirale des serveurs et des postes de travail

4C07 Maintien des comptes d'accès

4C08 Gestion des personnels critiques (vis-à-vis de la continuité des opérations)

D - Surveillance des actions sensibles

4D01 Surveillance des actions sensibles

05 Sécurité applicative et continuité de l'activité (05 App)

A - Contrôle de l'intégrité des données

5A01 Scellement des données sensibles

5A02 Protection de l'intégrité des données échangées

5A03 Contrôles permanents (vraisemblance...) sur les données et traitements

5A04 Contrôle des fonctions de calcul ou des programmes utilisateurs

B - Contrôle de la confidentialité des données

5B01 Chiffrement des échanges

5B02 Chiffrement des données stockées

C - Disponibilité des données

5C01 Gestion des contrôles d'accès aux données

D - Continuité de fonctionnement

5D01 Plans de continuité de l'activité

5D02 Plans de Reprise de l'Environnement de Travail (PRET)

06 Protection des postes de travail utilisateurs (06 Mic)

A - Protection des postes de travail

6A01 Contrôle d'accès au poste de travail

6A02 Travail en dehors des locaux de l'entreprise

B - Protection des données du poste de travail

6B01 Protection de la confidentialité des données contenues sur le poste de travail ou sur un serveur de données (disque logique pour le poste de travail)

6B02 Protection de l'intégrité des fichiers contenus sur le poste de travail ou sur un serveur de données (disque logique pour le poste de travail)

6B03 Sécurité de la messagerie électronique (courriels) et des échanges électroniques d'information

6B04 Sauvegarde des données utilisateurs stockées sur les postes de travail