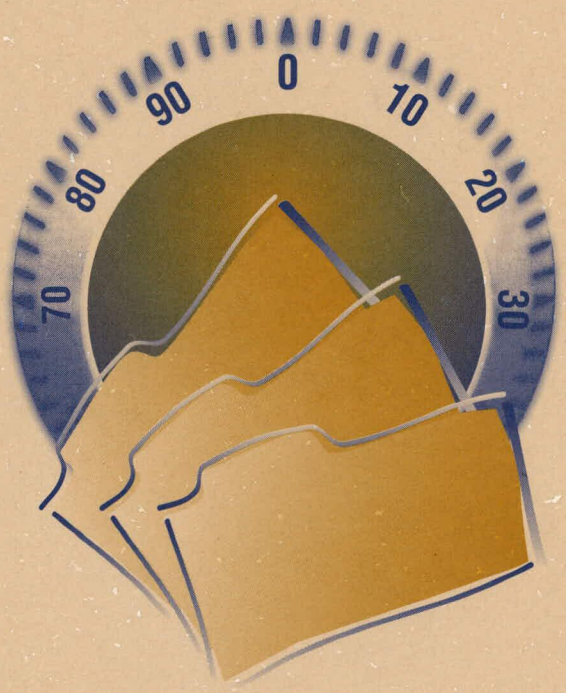


La sécurité de l'information

moi, je m'en occupe !

Québec
Ministère
des Transports

Ministère des Transports

Direction du Secrétariat général

Sécurité des actifs technologiques

Mai 2000

Table des matières

1. Introduction		1
2. État actuel de la sécurité à la Direction du Secrétariat général		2
2.1 Notation des facteurs de sécurité		5
2.2 Représentation graphique des facteurs		6
2.3 Vulnérabilité des facteurs étudiés		8
3. Analyse des risques		10
4. Choix des mesures prioritaires		11
5. Champ d'action		14
6. Conclusion		18
Annexe A	Références	22
Annexe B	Liste des participants	23
Annexe C	Notation des thèmes de sécurité	24
Annexe D	Notation du questionnaire	25
Annexe E	Méthode Delphi	27
Annexe F	Détail des mesures correctives	30
Source d'information		66

1. Introduction

Ce rapport s'inscrit dans le plan de mise en œuvre de la sécurité de l'information au ministère des Transports, qui a été entériné par le Comité de gestion en mars 1999. Lors du lancement de l'opération en octobre dernier visant à établir l'état de la situation au MTQ, le Comité ministériel de sécurité de l'information (CSI) a décidé de fournir un diagnostic pour chacune dees grandes unités administratives du Ministère afin de tenir compte de leurs particularités eu égard à la sécurité de leur information.

Le présent document constitue donc une première évaluation de l'état de la situation des actifs informationnels contenus dans les environnements technologiques de la Direction du Secrétariat général.

Les étapes couvertes sont :

- l'analyse de la situation actuelle (vulnérabilités);
- l'analyse des risques;
- l'indication du choix des mesures prioritaires à mettre en œuvre et du champ d'action privilégié pour assurer la disponibilité, l'intégrité et la confidentialité des ressources informationnelles de la direction.

La démarche utilisée est conforme aux principes de sécurité reconnus. Elle s'inspire des méthodes MARION* et MEHARI**, méthodes publiques d'analyse des risques et d'optimisation par niveau qui sont utilisées dans plus d'un millier d'organisations au niveau international (voir références à l'annexe A).

* MARION (méthodologie d'analyse des risques informatiques et d'optimisation par niveau) est l'une des méthodologies d'analyse de sécurité informatique les plus connues. Mise au point par le Club de la sécurité informatique français (CLUSIF) et privilégiée par la Commission d'accès à l'information du Québec (CAI), elle repose sur quelques grandes étapes : analyse de risque, expression du risque maximal admissible et calcul de la perte supportable par l'organisation, analyse des moyens de la sécurité, évaluation des contraintes, choix des moyens, orientations et avant-projet. ***Vocabulaire général de la sécurité informatique***, « Cahiers de l'Office de la langue française », Les Publications du Québec, 1996, page 21.

** MEHARI (méthode harmonisée d'analyse de risques informatiques) est une approche globale de la sécurité informatique dans des structures administratives décentralisées. Elle propose un cadre et une méthode qui garantit la cohérence des décisions prises par des unités jouissant d'une grande autonomie, et ce dans la complexité des systèmes distribués qui tendent à se généraliser, quelle qu'en soit l'étendue et la variété des composantes.

2. État actuel de la sécurité

L'analyse de **l'état actuel de la sécurité** effectuée à la Direction du Secrétariat général est fondée sur une enquête qui visait à déterminer les forces et particulièrement les faiblesses du dispositif en place. Cette étude a été réalisée au moyen d'un questionnaire de 204 questions adressées à des intervenants de trois catégories : gestionnaires, administrateurs(trices)-réseau et utilisateurs(trices). On retrouve à l'annexe B la liste des participants de la direction.

Cet exercice a permis d'inventorier et de quantifier de manière cohérente les mesures de sécurité de toute nature appliquées dans un contexte micro-réseau.

On obtient d'abord de cette analyse une notation, entre 0 et 4, des 27 facteurs de sécurité (voir 2.1) à partir de laquelle est présentée une représentation graphique des résultats obtenus par facteur (voir 2.2). On trouvera également, à l'annexe C, la notation obtenue pour chacun des 40 thèmes associés à ces facteurs.

Un autre graphique représente la vulnérabilité des facteurs étudiés (voir 2.3) en regard des risques analysés.

* * * *

L'état actuel de la sécurité est divisé en cinq sections : *l'appréciation générale de la sécurité* (facteurs 101, 102 et 103); *les facteurs socio-économiques* (facteur 201); *les principes généraux de la sécurité* (facteurs 301, 302, 303, 304, 305); *la sécurité logique et les télécommunications* (facteurs 401, 402, 403); *la sécurité de l'exploitation* (facteurs 501, 502, 503, 504, 505) et finalement *la sécurité dans le développement et les réalisations* (facteurs 601, 602, 603, 604). Voici une brève description de chaque facteur.

Appréciation générale de la sécurité

Facteur 101 Organisation, structure et fonctionnement des affaires; implication des gestionnaires, sensibilisation à la sécurité; évaluation des fonctions de l'organisation, des tâches et des assurances.

Facteur 102 Contrôles de gestion de l'existence de procédures écrites, du suivi des comptes sensibles et de la présence de détenteurs capables de classer leurs actifs technologiques.

Facteur 103 Procédures de sécurité et vérification de l'existence des procédures dans l'acceptation des documents, l'archivage de documents originaux, la sauvegarde et le caractère confidentiel des documents stratégiques localisés dans les bureaux.

Les facteurs sociaux économiques

Facteur 201 Évaluation, dans un sens général, de la satisfaction des employés.

Les principes généraux de sécurité

Facteur 301 Analyse de l'environnement physique de la sécurité, de l'entretien et des bâtiments où les ordinateurs sont localisés.

Facteur 302 Évaluation des contrôles d'accès physiques, de l'accès général aux bâtiments où les ordinateurs sont localisés, de l'entretien de systèmes d'accès, de la sensibilisation, de la formation et de l'information du personnel.

Facteur 303 Entretien des locaux et environnement statique.

Facteur 304 Directives de sécurité quant aux procédures identifiées et aux tests relatifs à ces procédures.

Facteur 305 Protection contre le feu et assurance que des mesures adéquates sont en place.

Facteur 306 Protection contre l'infiltration d'eau et mesures prises pour protéger les ordinateurs contre les dégâts d'eau.

Facteur 307 Vérification de la fiabilité du matériel quant à la disponibilité, le remplacement, la climatisation et la stabilité de l'installation électrique.

Facteur 308 Existence de procédures de secours et de sauvegarde.

Facteur 309 Existence de procédures de communication entre le personnel informatique et les utilisateurs.

Facteur 310 Formation du personnel.

Facteur 311 Vérification de l'existence d'un plan stratégique de sécurité informatique.

Sécurité logique et des télécommunications

Facteur 401 Vérification de la présence d'un système de contrôle d'accès logique permettant un suivi des accès.

Facteur 402 Sécurité des télécommunications qui traite de l'utilisation des mots de passe aussi bien que de l'usage des lignes spécifiques pour transporter l'information stratégique.

Facteur 403 Évaluation de l'existence de la sécurité au niveau des banques de données et des outils de l'administrateur de cette banque pour assurer l'intégrité, la continuité et la possibilité de récupération éventuelle des données.

Sécurité de l'exploitation

Facteur 501 Stockage et recouvrement des données avec procédures concernant l'archivage des documents et l'usage adéquat des moyens d'entreposage de l'information.

Facteur 502 Vérification de l'intégrité des données lors de la saisie et lors du traitement.

Facteur 503 Existence de procédures spécifiques pour sauvegarder et tester, dans le but éventuel de récupérer l'information lorsque cela est nécessaire.

Facteur 504 Analyse des procédures d'opérations (contrôles et documentation) au niveau du développement d'applications.

Facteur 505 Vérification de la présence de contrats pour le matériel, l'entretien des logiciels, et de l'existence d'un centre de support interne.

Sécurité dans le développement et les réalisations

Facteur 601 Procédures de « graduation » : tests avec utilisateurs et documentation adéquate.

Facteur 602 Existence d'une méthode d'analyse et de programmation ainsi que d'un plan pour chaque projet en développement.

Facteur 603 Analyse des conséquences d'un risque et des contrôles adéquats pour protéger l'information.

Facteur 604 Sécurité des progiciels et existence de contrats pour vérifier la capacité des fournisseurs à les exécuter selon les spécifications requises.

2.1 Notation des facteurs

Le tableau suivant présente la notation des 27 facteurs de sécurité pour la Direction du Secrétariat général. L'interprétation est effectuée de la façon suivante : 0 = faible, 3 = optimum, 4 = protection maximale. Pour être adéquatement protégée envers les 10 risques à l'étude, la direction doit atteindre la note optimale de 3. La note 4 indiquerait que des investissements additionnels seraient superflus pour ce ou ces facteurs.

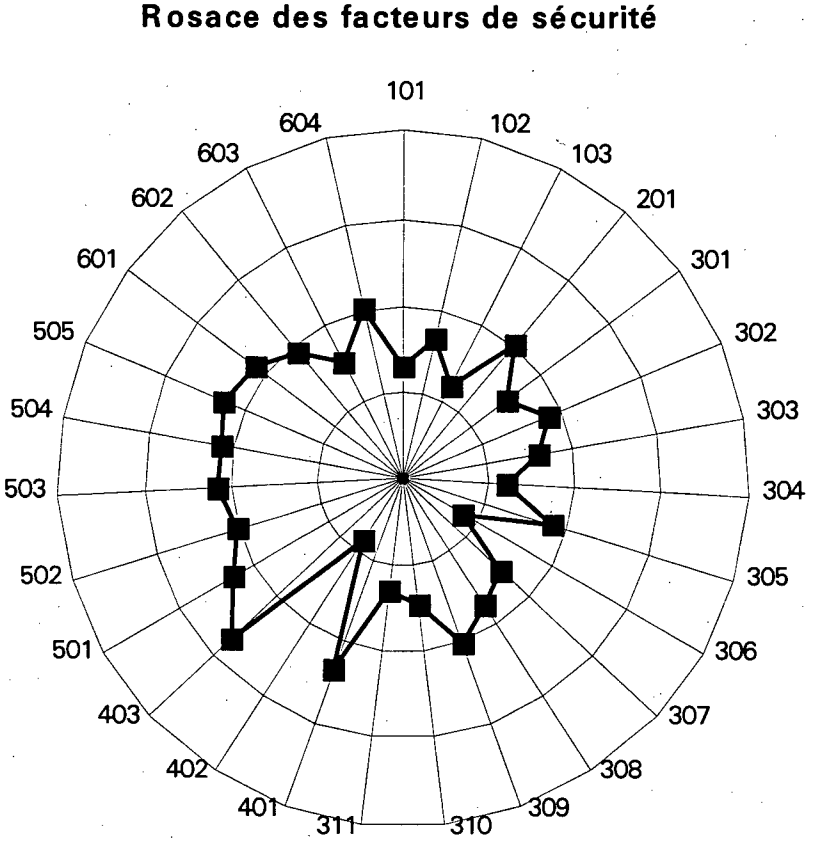
Facteurs	Description	Notation
101	L'organisation générale	1,30
102	Les contrôles permanents	1,67
103	La réglementation	1,20
201	Les facteurs socio-économiques	2,00
301	L'environnement de base	1,50
302	Les contrôles d'accès physiques	1,83
303	La pollution	1,60
304	Les consignes de sécurité physique	1,20
305	La sécurité incendie	1,80
306	La sécurité dégâts des eaux	0,80
307	La fiabilité de fonctionnement des matériels informatiques	1,55
308	Les systèmes et procédures de secours	1,73
309	Les protocoles utilisateurs-informaticiens	2,00
310	Le personnel	1,45
311	Les plans informatique et de sécurité	1,29
401	Les contrôles d'accès logique	2,34
402	La sécurité des télécommunications	0,85
403	La protection des données	2,70
501	L'archivage / désarchivage	2,27
502	La saisie et le transfert classique des données	2,00
503	La sauvegarde	2,15
504	Le suivi de l'exploitation	2,13
505	La maintenance	2,27
601	Les protocoles de graduation	2,16
602	Les méthodes d'analyse-programmation	1,89
603	Les contrôles programmés	1,50
604	La sécurité des progiciels	2,00

La notation de chaque question est présentée à l'annexe D.

Les résultats obtenus indiquent que certaines mesures de sécurité sont déjà en place dans le but d'assurer la protection des actifs technologiques de la Direction du Secrétariat général.

2.2 Représentation graphique des facteurs

La rosace suivante est une illustration graphique de la notation des facteurs pour la Direction du Secrétariat général. Elle met en évidence les points forts et les points faibles pour chacun des 27 facteurs étudiés.



La lecture se fait comme suit : le centre de la rosace vaut 0 et exprime une faiblesse, tandis que le cercle 3 représente l'objectif de cohérence / qualité (optimum). Le cercle 4, à l'extrémité extérieure de la représentation graphique, signifie que les facteurs dont la notation se situe entre le cercle 3 et le cercle 4 sont adéquatement protégés. Chaque rayon représente l'un des 27 facteurs de sécurité (de 101 à 604).

Bien qu'il soit tentant de le faire, il serait erroné de construire un plan de sécurité à partir du seul examen des points faibles apparaissant sur la rosace pour plusieurs raisons :

- on ne tient pas compte alors de leur incidence réelle sur les risques;
- les risques n'ont pas encore été évalués;
- relever, sans méthode, les facteurs les plus faibles ne garantit pas la cohérence (absence de failles) et donc la sécurité;
- on ne connaît pas encore les contraintes techniques et économiques qui permettraient de s'approcher d'une solution optimale.

2.3 Vulnérabilité des facteurs étudiés

Selon les résultats obtenus à partir de l'enquête et d'un tableau de vulnérabilités, dont les calculs sont préétablis dans l'utilisation des méthodes MARION et MEHARI, il est possible de déterminer la vulnérabilité de la Direction du Secrétariat général face aux trois secteurs de risques que sont les accidents, les erreurs et la malveillance.

On retrouvera ci-après la description de ces dix risques regroupés par secteur.

Accidents

01 Risques matériels : destruction partielle ou totale des matériels ou des supports informatiques et de leur environnement.
02 Vol, sabotage matériel : vol de petits matériels, supports informatiques et biens divers; sabotage physique.
03 Pannes et dysfonctionnement : arrêts ou baisses de service d'un centre informatique.

Erreurs

04 Erreurs de saisie, de transmission : pertes de temps, reprises, erreurs de lecture etc.; aiguillage, erreurs, parasites.
05 Erreurs d'exploitation : oubli ou écrasement d'un fichier ou d'une sauvegarde.
06 Erreurs de conception, de réalisation : non conformité des traitements; respect des délais de fabrication, de livraison.

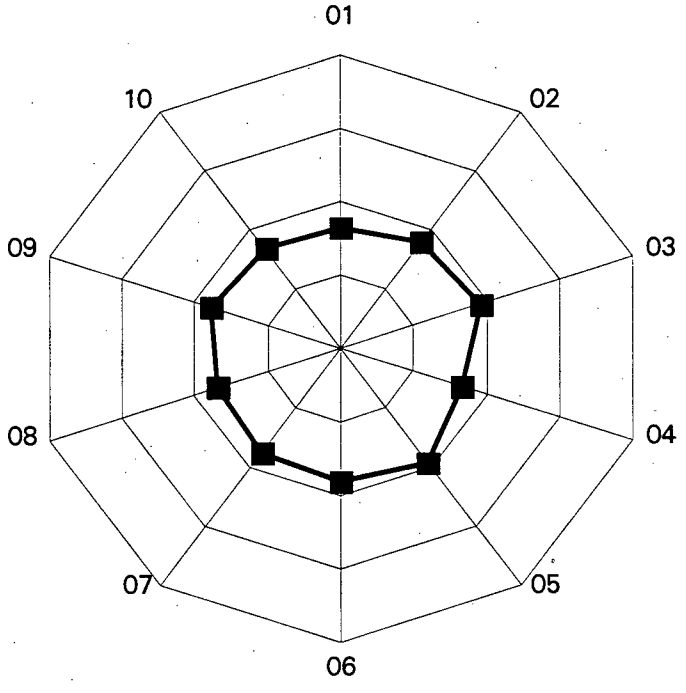
Malveillance

07 Fraude, sabotage immatériel : piratage, détournement d'avantages et ou de biens; bombes logiques, virus.
08 Indiscrétion, détournement : non respect déontologique, espionnage industriel.
09 Détournement de logiciel : copie illicite, plagiat.
10 Indisponibilité, départ de personnes : indisponibilité du personnel.

Le tableau qui suit indique la notation de la Direction du Secrétariat général en regard des dix risques étudiés.

Risque	Types de risques	Notation
01	Risques matériels	1,64
02	Vol, sabotage matériel	1,77
03	Pannes disfonctionnement	1,91
04	Erreurs de saisie, transmission	1,68
05	Erreurs d'exploitation	1,92
06	Erreurs de conception, réalisation	1,81
07	Fraude, sabotage immatériel	1,74
08	Indiscrétion, détournement	1,70
09	Détournement de logiciel	1,77
10	Grève, départ de personnes	1,67

Cette notation est transposée sur une rosace qui permet de visualiser la vulnérabilité de la Direction du Secrétariat général face à ces risques.



Cette rosace illustre la notation par risque comprise entre 0 et 4. Si la notation est supérieure à la valeur optimale (cercle 3), on en déduit que la direction générale a su mieux se protéger contre ce type de risque. L'interprétation se fait de la même façon que pour les facteurs, c'est-à-dire que le centre de la rosace vaut 0 (faible) et le cercle externe 4 (fort).

Puisque aucun des dix risques analysés ne rencontre la note optimale (3), les résultats démontrent que la Direction du Secrétariat général serait actuellement vulnérable si une ou plusieurs menaces venaient à se concrétiser.

3. Analyse des risques

L'**analyse des risques** a pour objectif l'évaluation des conséquences de la concrétisation éventuelle des 10 risques génériques reconnus en sécurité de l'information. Puisque tous les risques auxquels la Direction du Secrétariat général est exposée n'ont pas la même importance, il fallait identifier ceux qui peuvent avoir les conséquences les plus graves.

Tous les actifs informationnels ne peuvent être protégés contre tous les risques. Il importe de choisir en fonction des besoins réels et, en particulier, des besoins les plus pressants. Ces besoins ont été identifiés en évaluant les risques potentiels qui peuvent avoir les pires conséquences sur les opérations de la Direction du Secrétariat général. Cet exercice a permis de mettre en priorité les risques contre lesquels on doit d'abord se prémunir afin d'assurer la continuité des opérations, l'intégrité et la confidentialité de l'information.

Les dix risques évalués sont les mêmes que ceux décrits au point 2.3. Ces risques, si concrétisés, ont été évalués autant sous l'angle de l'**importance** que sur la probabilité d'**occurrence**. Le tableau qui suit montre :

- les risques analysés ainsi que leur numéro de référence;
- la notation de vulnérabilité obtenue lors de l'analyse de l'état actuel de la sécurité;
- la valeur relative accordée à chacun des risques et donc l'ordre de priorité dans lequel ils doivent être contrés.

	Risques	*Notation*	*Importance*	*Occurrence*	*Total*	*Rang*
01	Risques matériels	1,64	44	29	73	3
02	Vol sabotage	1,77	31	18	49	7
03	Pannes et dysfonctionnement	1,91	25	50	75	2
04	Erreurs de saisie	1,68	10	42	62	5
05	Erreurs d'exploitation	1,92	21	29	60	6
06	Erreurs de conception	1,81	43	25	68	4
07	Fraude et sabotage	1,74	45	49	94	1
08	Indiscrétion et détournement	1,70	35	5	40	8
09	Détournement de logiciel	1,77	0	4	4	10
10	Grève et départ de personnel	1,67	16	14	30	9

La méthode Delphi a été utilisée pour en arriver à ce pointage (voir annexe E). Il s'agissait d'indiquer sur une grille prévue à cet effet la préférence d'un risque par rapport à un autre. Au terme de cet exercice, le groupe de travail a pu dégager les risques qui lui apparaissaient les plus importants, c'est-à-dire ceux qui peuvent compromettre l'atteinte des objectifs de la Direction du Secrétariat général advenant leur concrétisation.

4. Choix des mesures prioritaires

Les besoins de sécurité de la Direction du Secrétariat général doivent maintenant être établis en fonction des risques les plus importants. L'**analyse de l'état actuel** a fait ressortir les faiblesses de la sécurité déjà en place. Il reste à voir à quels facteurs seront appliquées les mesures requises pour faire face à la concrétisation éventuelle de ces risques.

Les méthodes MARION et MEHARI ont développé, sur la base de statistiques compilées pendant au moins une décennie, une grille de détermination des facteurs sur lesquels il faut agir prioritairement, afin de contrer les risques rangés suivant leur importance et la possibilité de leur occurrence lors de l'**analyse de risques**.

Cette grille a donc été utilisée pour déterminer les facteurs à corriger pour chacun des risques à contrer par la Direction du Secrétariat général. Pour en arriver à un résultat efficace, il faut corriger d'abord les trois premiers facteurs associés à chacun des risques en tenant compte du résultat obtenu par la direction.

Risques	Correction des facteurs par ordre d'importance																				
1	**305**	**301**	**308**	503	304	307	101	306	303	311	505	201	501								
2	**302**	**505**	**308**	305	301	503	310	304	311	101	306	401	307	201	501	103					
3	**308**	**401**	**505**	307	503	301	504	101	303	306	304	311	310	501	403						
4	**603**	**504**	**102**	103	308	401	503	501	402	101	301	309	310	403	502	505	311	306	302	303	201
5	**504**	**503**	**401**	102	308	402	310	103	403	501	101	311	301	309	502	505	201	601			
6	**601**	**602**	**311**	310	103	402	309	102	101	604	503	603	504	401	403	501	201				
7	**603**	**402**	**503**	401	102	602	103	504	601	403	308	310	302	309	101	501	201	502	311		
8	**402**	**401**	**103**	403	102	302	503	603	601	504	310	101	604	501	309	201	502	311	301		
9	**302**	**604**	**402**	503	401	103	504	310	602	101	403	102	201	603	309	501					
10	**310**	**308**	**503**	101	504	103	604	311	302	102	201	309	501	301	402	401	403				

Les facteurs à corriger sont donc présentés en suivant l'ordre de priorité établi (voir tableau de la section 3) à l'aide de la méthode Delphi. Aussi bien pour les facteurs que pour les risques, on retrouve entre parenthèses la notation de la Direction du Secrétariat général apparaissant sur les deux rosaces respectives présentées aux sections 2.2 et 2.3. Rappelons encore que la note 3 est la note recherchée. Une note allant de 0 à 2,9 indique qu'il faut améliorer la situation pour atteindre un niveau acceptable de protection.

1. Facteurs à corriger pour contrer le risque 07 - Fraude et sabotage (1,74

603 Les contrôles programmés (1,50)

402 La sécurité des télécommunications (0,85)

503 La sauvegarde (2,15)

2. Facteurs à corriger pour contrer le risque 03 - Pannes et dysfonctionnements (1,91)

308 Les systèmes et procédures de secours (1,73)

401 Les contrôles d'accès logique (2,34)

505 La maintenance (2,27)

3. Facteurs à corriger pour contrer le risque 01 - Risques matériels (1,64)

305 La sécurité incendie (1,80)

301 L'environnement de base (1,50)

308 Les systèmes et procédures de secours (1,73)

4. Facteurs à corriger pour contrer le risque 06 - Erreurs de conception (1,81)

601 Les protocoles de graduation (2,16)

602 Les méthodes d'analyse-programmation (1,89)

311 Les plans informatique et de sécurité (1,29)

5. Facteurs à corriger pour contrer le risque 04 - Erreurs de saisie, de transmission (1,68)

603 Les contrôles programmés (1,50)

504 La sécurité de l'exploitation (2,13)

102 Les contrôles permanents (1,67)

6. Facteurs à corriger pour contrer le risque 05 - Erreurs d'exploitation (1,92)

504 La sécurité de l'exploitation (2,13)

503 La sauvegarde (2,15)

401 Les contrôles d'accès logique (2,34)

7. Facteurs à corriger pour contrer le risque 02 - Vol et sabotage (1,77)

302 Les contrôles d'accès physiques (1,83)

505 La maintenance (2,27)

308 Les systèmes et procédures de secours (1,73)

8. Facteurs à corriger pour contrer le risque 08 - Indiscrétion et détournement (1,70)

402 La sécurité des télécommunications (0,85)

401 Les contrôles d'accès logique (2,34)

103 La réglementation (1,20)

9. Facteurs à corriger pour contrer le risque 10 - Grève et départ de personnel (1,67)

310 Le personnel (1,45)

308 Les systèmes et procédures de secours (1,73)

503 La sauvegarde (2,15)

10. Facteurs à corriger pour contrer le risque 09 - Détournement de logiciel (1,77)

302 Les contrôles d'accès physiques (1,83)

604 La sécurité des progiciels (2,00)

402 La sécurité des télécommunications (0,85)

Les corrections à mettre en place pour les dix risques, rangés en fonction des besoins spécifiques de la Direction du Secrétariat général, nous montrent la récurrence de certains facteurs à rétablir. Ainsi, le facteur 603 (Les contrôles programmés) est le premier facteur devant être amélioré. Il revient dans les cas du premier et cinquième risques les plus menaçants pour la direction (risques 07 et 04). Il est donc évident que les mesures reliées à l'optimisation du facteur 603 devront être mises en place rapidement à la Direction du Secrétariat général, d'autant plus que la compilation des résultats du questionnaire indique une notation de 1,50 pour ce facteur, ce qui signifie que des efforts doivent être consentis à court terme pour atteindre la cote optimale de 3. Viennent ensuite les facteur 503 (La sauvegarde) et 308 pour les risques 07, 03, 01, 05 et 02. Avec une notation de 1,73, il faudra certainement porter une attention particulière au facteur 308. Et ainsi de suite...

On comprend donc comment fonctionnent les méthodes utilisées.

Il ne faut pas oublier non plus le facteur 402 (La sécurité des télécommunications) pour lequel les résultats indiquent une notation ministérielle très faible de 0,85. Avec l'utilisation sans cesse grandissante de l'Internet et du courrier électronique, en plus de l'avènement du télétravail et le recours aux accès commutés, il faut améliorer à tout prix ce facteur pour contrer le risque 07, qui menace la Direction du Secrétariat général ainsi que le réseau desservant l'ensemble des unités administratives du ministère des Transports. L'enjeu est majeur et il s'agit d'une responsabilité de la DTI.

On sait en outre qu'au niveau gouvernemental la protection de la confidentialité est une priorité et que la responsabilité ministérielle de gestion de cette priorité incombe au titulaire du Secrétariat général. Là encore, c'est la correction du facteur 402 qui a l'incidence positive la plus notoire pour prévenir l'occurrence de ce type de risque. Le gouvernement veut en effet se prémunir contre toutes les « fuites » qui pourraient entacher la réputation des ministères et organismes.

La Direction du Secrétariat général aura également à collaborer à l'amélioration des facteurs 103 (La réglementation), 304 (Les consignes de sécurité), 306 (La sécurité dégât des eaux) et 311 (Les plans informatiques et de sécurité), car la notation de ces facteurs, qui se situe près de la cote 1,00, doit être sensiblement améliorée à court terme.

Telle est la logique de la démarche. Le champ d'action propre au contexte de la Direction du Secrétariat général est décrit dans la prochaine section.

5. Champ d'action

La section précédente a identifié et classé dans un ordre décroissant d'importance les facteurs à corriger afin d'atteindre, éventuellement, un niveau optimum de sécurité à la Direction du Secrétariat général. Certaines parmi les actions énumérées ci-après relèvent de la responsabilité de la DTI (ex. : les contrôle programmés, la sécurité des télécommunications). D'autres feront l'objet de mesures applicables à l'ensemble des unités administratives du ministère des Transports (ex. : plan de secours). La partie suivante, qui est la **conclusion** de ce rapport, s'en tient plus strictement aux priorités d'action propres à la direction.

Cependant, comme la sécurité de l'information est une affaire ministérielle, voici les mesures mises en évidence par les répondants de la Direction du Secrétariat général comme devant être prises en compte dans l'élaboration du premier **Plan ministériel de sécurité de l'information**. Elles ont comme caractéristique de concerner à la fois le Ministère et la direction. Elles devront être évaluées dans le cadre du Plan pour en déterminer la faisabilité, les coûts, les efforts de réalisation, les ressources impliquées, les biens livrables, les échéanciers, etc.

Les contraintes humaines, techniques et financières devront aussi être prises en compte dans le choix des mesures à mettre en place, tant à la direction qu'au niveau ministériel. Enfin, à court terme, les mesures ayant un impact positif important sur la sécurité à un coût moindre auront priorité sur les autres mesures.

* * * *

Voici, dans l'ordre, les mesures privilégiées par les répondants de la direction, sans tenir compte pour l'instant de qui relèvera la responsabilité de leur mise en œuvre. L'ordre de priorité fut établi à la section 4, intitulée **Choix des mesures prioritaires,** et reflète fidèlement la compilation des résultats obtenus à la Direction du Secrétariat général.

- **(603) Les contrôles programmés – 1,50**

Lors du développement d'applications, on doit s'assurer qu'il y a une étude quantitative des conséquences d'erreur ou d'action malveillante sur chaque type de données stratégiques.

- **(402) La sécurité des télécommunications – 0,85**

Toutes les communications, sans exception, doivent passer par un serveur. L'accès aux fonctions de communication doit être restreint et ces accès doivent être enregistrés.

Les communications stratégiques doivent disposer d'un système spécifique de sécurité d'accès logique et, de plus, être chiffrées.

- **(503) La sauvegarde – 2,15**

Il faut réaliser et mettre à la disposition des usagers un plan de sauvegarde des informations sur support électronique. Ce plan doit fournir, entre autres, des règles strictes mentionnant le nombre de générations, la périodicité, le lieu et la durée de stockage des sauvegardes, ainsi que des procédures (techniques, utilisateurs) de reprise précisant notamment la conduite à tenir.

- **(308) Plan de secours – 1,73**

Il faut se doter d'un plan de secours pour l'ensemble des infrastructures technologiques, plus spécifiquement pour celles de la Direction du Secrétariat général, lequel tiendra compte du délai d'indisponibilité maximum admissible pour chacune de ces infrastructures.

- **(401) Les contrôles d'accès logique – 2,34**

Il faut qu'il y ait une meilleure utilisation des mots de passe, autant pour les données courantes que pour les données stratégiques. Les accès par le personnel doivent être systématiquement suivis et contrôlés.

- **(505) La maintenance – 2,27**

Un centre technique de support maintenance, interne ou externe, doit fournir une assistance téléphonique rapide. On doit aussi évaluer la possibilité de se prévaloir de contrats de maintenance pour les équipements, périphériques et logiciels. Les responsabilités des créateurs et utilisateurs de programmes doivent être clairement définies. L'autorisation, par exemple, de deux administrateurs LAN (*Local Area Network* ou réseau local) peut être rendue indispensable pour certaines opérations critiques.

- **(305) La sécurité incendie – 1,80**

Les utilisateurs doivent faire en sorte que les documents ou supports informatiques contenant des informations stratégiques, stockées dans leurs bureaux, soient entreposés dans des meubles réfractaires.

- **(301) L'environnement de base – 1,50**

Lors de l'installation d'infrastructures technologiques, on doit tenir compte des moyens de sécurité appropriés pour contrer les nuisances liées aux désastres naturels et particulièrement ceux reliés à l'eau.

Il faut aussi procéder à une vérification périodique des installations électriques afin de s'assurer, entre autres, que la prise de terre est adéquate.

- **(601) Les protocoles de graduation – 2,16**

Lors de développement d'applications, il faut séparer l'environnement de développement de l'environnement test et de l'environnement exploitation. On doit procéder à des tests de validation sur un appareil dédié en ce qui concerne les logiciels, tout en s'assurant que la réception finale soit confiée au détenteur lui-même.

- **(602) Les méthodes d'analyse-programmation – 1,89**

Chaque projet doit faire l'objet d'un avant-projet et d'un cahier des charges élaborés avec le concours des utilisateurs, en liaison avec le représentant des tiers.

La conception (et la réalisation) de l'application doit intégrer les spécifications de sécurité qui résultent elles-mêmes d'une analyse méthodique et formelle des menaces potentielles.

- **(311) Plans informatiques et de sécurité – 1,29**

Le plan de sécurité des systèmes d'information doit couvrir le domaine des micros : analyse des vulnérabilités et des menaces, solutions, organisation de la sécurité.

- **(504) La sécurité de l'exploitation – 2,13**

Le ministère des Transports doit se doter de procédures d'exploitation permettant, entre autres, la « gestion des résidus » (effacement physique des zones mémoires contenant des données sensibles). À ce propos, une mise à jour de la directive 2.5.1 du Manuel administratif a été apportée en avril 2000 en conformité avec le CT 193953 du Conseil du trésor.

- **(102) Les contrôles permanents - 1,67**

Chaque fonction stratégique doit avoir une unité administrative ou une personne nommément désignée pour jouer le rôle de « détentrice des informations », et chargée à ce titre de la classification des informations ainsi que de la définition des règles et autorisations d'utilisation de ces informations.

- **(302) Les contrôles d'accès physiques – 1,83**

Il faut implanter un système de contrôle systématique des accès aux bâtiments et sensibiliser le personnel contrôlant ces accès au risque de vol de petits matériels ou de sortie illicite de matériel.

Des procédés anti-vol doivent être mis en place pour les petits matériels et le contrôle de la sortie de systèmes portables.

Les bureaux renfermant des petits matériels et des supports informatiques doivent pouvoir fermer à clé (serrure certifiée) et effectivement être fermés à clé.

- **(103) La réglementation – 1,20**

Le ministère des Transports doit établir des règles écrites de sécurité et de confidentialité concernant les documents et supports (disquettes) stratégiques situés dans les bureaux.

On doit aussi prendre en compte la possibilité de destruction totale d'informations stratégiques sur support informatique et mettre en place des procédures systématiques de rétention des documents de base à des fins de reconstitution.

Dans les circuits d'information où certains traitements sont réalisés sur les micro-ordinateurs, toute pièce administrative ou comptable doit être « marquée » (initiales et/ou signatures identifiables) par les personnes qui la traitent. Les doubles des pièces administratives ou comptables doivent être annulés dès réception pour éviter des duplications d'enregistrements sur les postes de travail.

- **(310) Le personnel – 1,45**

Le ministère des Transports doit procéder à une sensibilisation de l'ensemble du personnel aux problèmes de sécurité. Des plans de formation seront conçus également pour toutes les catégories d'employés du Ministère. On doit mettre en place une information déontologique et juridique concernant la propriété des programmes internes et progiciels externes.

On doit, de plus, s'assurer qu'il y ait une documentation complète des applications, systèmes et matériels stockés dans un lieu protégé. Les utilisateurs doivent être informés des symptômes, puis des procédures à prendre pour contrer l'effet des virus informatiques sur leur environnement. Ils doivent être informés des règles précises et limitatives pour l'utilisation de commandes et outils dangereux.

- **(604) La sécurité des progiciels – 2,00**

Les logiciels d'applications acquis ou développés pour le ministère des Transports doivent d'abord être testés et il faut aussi s'assurer de récupérer les programmes sources du fournisseur. Une documentation adéquate et un minimum de formation au démarrage sont requis et on doit effectuer le choix en tenant compte de la capacité des fournisseurs à maintenir et à faire évoluer les produits.

6. Conclusion

Les forces et les faiblesses propres à la Direction du Secrétariat général, en matière de protection de ses actifs technologiques, ont été identifiées. L'analyse des risques a ensuite démontré l'importance qu'aurait la concrétisation de ces risques sur ses opérations.

Avec une notation se situant près de la cote de 1,00, une préoccupation particulière doit être accordée aux facteurs 101, 103, 304, 306 et 311.

Quant au facteur ministériel 402, une amélioration déterminante doit être mise en œuvre au niveau ministériel dès maintenant, compte tenu du fait que la « boîte à outils » qu'est la SI constitue l'instrument essentiel pour assurer aussi bien la protection des renseignements personnels que celle de l'ensemble des opérations du Ministère. Et cela, eu égard aux trois fonctions essentielles de l'information numérique : la **disponibilité**, l'**intégrité** (le MTQ gère un nombre considérable de données dont la conservation intégrale assurera la continuité nécessaire à l'accomplissement de sa mission) et la **confidentialité** dont on n'ignore plus le caractère stratégique. À ces fonctions s'ajouteront bientôt l'**authentification** et l'**irrévocabilité** dans le cadre imminent de l'implantation de l'infrastructure à clés publiques du gouvernement (ICPG) destiné à sécuriser les transactions électroniques.

On peut donc préciser les orientations et l'ordre de priorité à accorder aux mesures à mettre en place pour sécuriser les actifs technologiques de la Direction du Secrétariat général. Le choix de ces mesures devra toutefois tenir compte des contraintes potentielles : humaines, techniques et financières. Enfin, les mesures retenues qui feront l'objet de projets concrets seront inscrites au premier ***Plan ministériel de la sécurité de l'information***.

* * * *

Les principales recommandations pour la Direction du Secrétariat général touchent les volets suivants dans un ordre décroissant d'importance :

- **Mise en place de contrôles programmés (603)**

Responsabilité ministérielle : La DTI devra fournir aux détenteurs les moyens nécessaires à la protection des données stratégiques.

Responsabilité de la direction : La Direction du Secrétariat général doit d'abord et avant tout identifier les données stratégiques sous sa juridiction et procéder lors du développement d'applications à une étude quantitative des conséquences d'erreur ou d'action malveillante.

- **Sécurité des télécommunications (402)**

Responsabilité ministérielle : La DTI doit voir à ce que toutes les communications, sans exception, soient soumises à une gestion adaptative de la sécurité des réseaux (ASM – *Adaptative Security Management*) et s'assurer que les accès aux fonctions de communication soient restreints et enregistrés par l'entremise d'un système spécifique de sécurité d'accès logique.

Responsabilité de la direction : Après identification de ses communications stratégiques, la Direction du Secrétariat général doit utiliser un système spécifique de sécurité d'accès logique, et devra bientôt chiffrer ces informations.

- **Plan de sauvegarde des informations sur support électronique (503)**

Responsabilité ministérielle : La DTI verra à l'implantation d'un plan de sauvegarde ministériel.

Responsabilité de la direction : Il est nécessaire de réaliser un plan de sauvegarde à la Direction du Secrétariat général pour les actifs informationnels gérés localement.

- **Élaboration d'un plan de secours de l'information électronique (308)**

Responsabilité ministérielle : Le ministère des Transports doit se doter d'un plan de secours pour l'ensemble de ses infrastructures technologiques et l'intégrer au ***Plan ministériel de sécurité de l'information***.

Responsabilité de la direction : Il est requis de procéder à un inventaire des actifs technologiques de la Direction du Secrétariat général. Ceux gérés par la DTI et ceux gérés localement par la direction. Il faut de plus déterminer la durée d'indisponibilité maximum acceptable pour chacun de ces actifs. Les travaux préparatoires au bogue de l'an 2000 (plans de contingence) constituent un excellent point de départ pour cet inventaire et cette réflexion. Il faut savoir quoi protéger et la prochaine étape sera justement d'évaluer le degré de protection requise pour chacun des actifs technologiques de la direction en fonction des critères de disponibilité, intégrité et confidentialité propres à ces systèmes d'information.

- **Programme de sensibilisation : mots de passe et déontologie (401)**

Responsabilité ministérielle : Le ministère des Transports réalisera un programme de sensibilisation à l'intention des employés qui sera lancé à l'automne 2000, lequel couvrira entre autres l'utilisation des mots de passe. Le Ministère fournira en outre, dans le cadre du ***Plan ministériel de sécurité de l'information***, les outils nécessaires pour contrôler les accès aux données.

Responsabilité de la direction : Les détenteurs et utilisateurs doivent dès maintenant être spécifiquement sensibilisés à l'utilisation appropriée des mots de passe. Du matériel sera fourni pour informer le personnel, dans le cadre du programme de sensibilisation, à propos des aspects déontologique et juridique touchant la sécurité de l'information. Des efforts particuliers doivent être consentis pour améliorer fortement la sensibilisation du personnel, d'autant plus que cette mesure n'est pas très coûteuse et que l'expérience a démontré que la sensibilisation est le meilleur atout pour assurer la sécurité de l'information. Des initiatives propres à la direction elle-même sont également très souhaitables en cette matière.

- **Maintenance (505)**

Responsabilité ministérielle : Un centre technique de support maintenance doit être mis en place pour fournir une assistance téléphonique rapide. Il est requis d'évaluer la nécessité de se doter de contrats de maintenance pour les infrastructures technologiques du ministère des Transports.

Responsabilité de la direction : Les détenteurs auront à évaluer la nécessité de se prévaloir de contrats de maintenance pour les équipements, périphériques et logiciels sous leur juridiction.

- **Sécurité de l'exploitation (504)**

Responsabilité ministérielle : La Direction des contrats et des ressources matérielles a officialisé les procédures d'exploitation permettant, entre autres, l'effacement physique des zones mémoires contenant des données sensibles.

La DTI doit informer les utilisateurs des symptômes, puis des procédures à prendre pour contrer l'effet des virus informatiques sur leurs environnements respectifs. Les utilisateurs seront aussi informés des règles précises et limitatives pour l'utilisation de commandes et outils dangereux.

Responsabilité de la direction : Les détenteurs doivent s'assurer d'avoir une documentation complète des applications, systèmes et matériels stockés dans un lieu protégé.

Les utilisateurs doivent prendre les mesures nécessaires pour contrer l'effet des virus informatiques sur leur environnement et appliquer les règles précises et limitatives dans l'utilisation de commandes et outils dangereux.

- **Nomination d'un détenteur pour chaque fonction stratégique (102)**

Responsabilité ministérielle : Un registre d'autorité sera réalisé et maintenu à jour. Ce sera la liste de toutes les unités et des actifs informationnels placés sous leur responsabilité.

Responsabilité de la direction : Les détenteurs(trices) d'actifs informationnels doivent être identifié(e)s. Ce sont ceux ou celles pour qui les actifs informationnels ont été créés ou acquis afin de mener les opérations de la Direction du Secrétariat général. En même temps que l'évaluation des actifs en fonction des critères de disponibilité, intégrité et confidentialité, la responsabilité de chacun de ces actifs sera attribuée à un détenteur(trice), qu'il s'agisse d'une personne ou d'une unité administrative qui exploite cet actif informationnel.

D'autres mesures se grefferont sans aucun doute à celles qui viennent d'être mises en évidence dans le cadre du futur ***Plan ministériel de sécurité de l'information***. Il suffit de penser aux procédures de graduation, aux méthodes d'analyse-programmation, aux plans informatiques et de sécurité (architecture), sans oublier l'environnement de base, la réglementation, les contrôles d'accès physique et la sécurité des progiciels. Les quelques mesures énumérées ci-haut permettront à la Direction du Secrétariat général de s'engager plus avant dans la sécurité de son information.

Annexe A

Références

Albany International

Assurances Vie Desjardins

Bombardier

Centre Hospitalier Robert-Giffard

Confédération des Caisses Populaires Desjardins

Culinar

Donohue

Fédération des Caisses Populaires Desjardins

Gaz Métropolitain

Gouvernement du Québec, (200 ministères et organismes)

Hydro Québec

Pêches et Océans Canada

Société de l'Assurance Automobile du Québec

Steikeman Elliott

Université Laval

Ville de Sainte-Foy

etc.

Alcatel TITN Answare

A.P.S.A.D.

Banque de France

Bull S.A.

Caisse Nationale de Crédit Agricole

CAP SESA

Dassault Electronic

Framatome

France Telecom

Gan Industrie Services

Groupe Henner

Hewlett Packard France

I.B.M. France

La France des Jeux

La Poste

Ministère de l'Intérieur

Rhone Poulenc

Shell

3M France

Thompson – CSF

etc.

<u>Pays utilisateurs de la méthode MARION</u>

Afrique du Sud, Argentine, Belgique, Espagne, France, Italie, Maroc, Portugal, Canada (Québec), Russie, Suisse, Tunisie.

Annexe B

Liste des participants

M. François Beaudry

M. Gilles Brochu

M. Jacques Brouard

M. Éric Cantin

Mme Linda Clermont

M. Berchmans Couillard

M. Bertrand Fournier

M. Réal Gagnon

Mme Marthe Gingras

Mme Joyce Gonthier

M. Pierre Lefrançois

M. Richard Normand

M. Pierre Perron

Annexe C

Facteur	Thème	Libellé	Général
101		**L'organisation générale**	**1,30**
	1	Définitions des responsabilités	1,47
	2	Organisation de la sécurité	1,15
102		**Les procédures de sécurité**	**1,67**
	1	Procédures	1,73
	2	Structure des responsabilités	1,63
103		**La réglementation**	**1,20**
	1	Règles de contrôle	1,31
	2	Gestion des pièces justificatives	1,00
201		**Les facteurs socio-économiques**	**2,00**
	1	Les facteurs socio-économiques	2,00
301		**L'environnement de base**	**1,50**
	1	Sécurité du bâtiment et de l'environnement	1,36
	2	Sécurité physique de base ST/LAN	1,47
302		**Les contrôles d'accès physique**	**1,83**
	1	Contrôle d'accès	2,14
	2	Intrusion	1,00
303		**La pollution**	**1,60**
	1	Poussières et inflammabilité	1,33
	2	Electricité statique	2,00
304		**Les consignes de sécurité physique**	**1,20**
	1	Consignes de sécurité	1,20
305		**La sécurité incendie**	**1,80**
	1	Détection automatique	2,00
	2	Extinction	1,33
306		**La sécurité des dégâts des eaux**	**0,80**
	1	Prévention	0,80
307		**La fiabilité de fonctionnement des matériels infor.**	**1,55**
	1	Qualité du système	1,60
	2	Environnement	1,40
308		**Les systèmes et procédures de secours**	**1,73**
	1	Moyens de secours	1,73
309		**La cohérence des systèmes**	**2,00**
	1	Cohérence des systèmes	2,00
310		**Formation du personnel**	**1,45**
	1	Formation du personnel	1,45
311		**L'architecture**	**1,29**
	1	Plan, procédures informatiques et sécurité	1,83
	2	Architecture	1,00
401		**La sécurité logique de base**	**2,34**
	1	Identification-Authentification	2,26
	2	Contrôle d'accès	2,39
402		**La sécurité de communications**	**0,85**
	1	Sécurité générale LAN/WAN	0,87
403		**La protection et le contrôle des données**	**2,70**
	1	Protection des données	2,70
501		**L'archivage / désarchivage**	**2,27**
	1	Procédures et gestion des supports	2,27
502		**La saisie et le transfert classiques des données**	**2,00**
	1	Transfert sécurisé des données	2,00
503		**La Sauvegarde**	**2,15**
	1	Sauvegarde	2,15
504		**Le suivi de l'exploitation**	**2,13**
	1	Sécurité générale de l'exploitation	1,86
	2	Sécurité spécifique d'exploitation LAN	2,29
	3	Sécurité virus	2,24
505		**La maintenance**	**2,27**
	1	Contrats	2,27
601		**Les protocoles de graduation**	**2,16**
	1	Procédure de graduation	2,80
	2	Graduation des applications	2,00
602		**Les méthodes d'analyse programmation**	**1,89**
	1	Méthodes d'analyse programmation	1,89
603		**Les contrôles programmés**	**1,50**
	1	Choix et cohérence des contrôles	1,33
	2	Contrôles programmés	1,75
604		**La sécurité des progiciels**	**2,00**
		Progiciels	2,00

Annexe D

Facteur No.	Question	Notation	Pondération	Question pondérée	Notation thème	Notation facteur
101	01	2	2	4		
	02	2	3	6		
	03	2	1	2		
	04	3	2	6		
	05	1	2	2		
	06	1	2	2		
	07	0	2	0	1,47	
	08	2	4	8		
	09	1	7	7		
	10	1	5	5		
	11	1	2	2		
	12	1	4	4		
	13	1	3	3		
	14	1	1	1	1,15	
Total 101			40	52		1,30
102	01	1	3	3		
	02	2	8	16	1,73	
	03	1	5	5		
	04	2	7	14		
	05	2	2	4		
	06	2	4	8		
	07	0	1	0	1,63	
Total 102			30	50		1,67
103	01	1	5	5		
	02	1	6	6		
	03	2	5	10	1,31	
	04	1	2	2		
	05	1	7	7	1,00	
Total 103			25	30		1,20
201	01	2	5	10		
	02	2	2,5	5		
	03	2	2,5	5	2,00	
Total 201			10	20		2,00
301	01	3	2	6		
	02	1	2	2		
	03	1	2	2		
	04	1	1	1		
	05	1	2	2		
	06	1	2	2	1,36	
	07	2	1	2		
	08	2	3	6		
	09	2	2	4		
	10	2	2	4		
	11	2	3	6		
	12	0	5	0		
	13	4	1	4		
	14	2	1	2		
	15	2	1	2	1,47	
Total 301			30	45		1,50
302	01	2	2	4		
	02	3	3	9		
	03	3	3	9		
	04	3	2	6		
	05	2	4	8		
	06	2	3	6		
	07	1	2	2		
	08	1	3	3	2,14	
	09	1	3	3		
	10	1	5	5	1,00	
Total 302			30	55		1,83
303	01	1	2	2		
	02	2	1	2	1,33	
	03	2	2	4	2,00	
Total 303			5	8		1,60
304	01	1	1	1		
	02	2	1	2		
	03	1	3	3	1,20	
Total 304			5	6		1,20
305	01	2	6	12		
	02	2	4	8	2,00	
	03	2	6	12		
	04	2	4	8		
	05	1	5	5	1,33	
Total 305			25	45		1,80
306	01	2	2	4		
	02	0	3	0	0,80	
Total 306			5	4		0,80
307	01	3	3	9		
	02	0	3	0		
	03	1	3	3		
	04	2	3	6		
	05	2	3	6	1,60	
	06	1	2	2		
	07	1	1	1		
	08	2	2	4	1,40	
Total 307			20	31		1,55
308	01	2	25	50		
	02	1	7	7		
	03	2	3	6		
	04	2	5	10		
	05	1	5	5	1,73	
Total 308			45	78		1,73
309	01	2	10	20		
	02	2	5	10	2,00	
Total 309			15	30		2,00
310	01	2	3	6		
	02	2	2	4		
	03	1	6	6		
	04	2	4	8		
	05	1	2	2		
	06	1	3	3	1,45	
Total 310			20	29		1,45
311	01	2	8	16		
	02	1	2	2		
	03	2	2	4	1,83	
	04	1	1	1		
	05	1	3	3		
	06	1	2	2		
	07	1	11	11		
	08	1	2	2		
	09	2	2	4		
	10	0	2	0	1,00	
Total 311			35	45		1,29
401	01	1	10	10		
	02	3	10	30		
	03	3	2	6		
	04	2	3	6		
	05	3	3	9		
	06	2	3	6		
	07	2	3	6		
	08	3	2	6		
	09	3	3	9	2,26	
	10	3	15	45		
	11	2	10	20		
	12	1	4	4		
	13	2	5	10		
	14	3	3	9		
	15	3	3	9		
	16	2	3	6		
	17	2	4	8		
	18	2	4	8		
	19	3	3	9		
	20	3	3	9		
	21	2	1	2		
	22	3	1	3		
	23	2	2	4	2,39	
Total 401			100	234		2,34

402	01	1	11	11		
	02	1	5	5		
	03	0	5	0		
	04	0	2	0		
	05	3	1	3		
	06	3	1	3		
	07	0	2	0		
	08	0	2	0		
	09	1	2	2		
	10	0	1	0		
	11	0	2	0		
	12	2	5	10	0,87	
	13	3	10	30		
	14	0	10	0		
	15	0	3	0		
	16	0	1	0		
	17	0	2	0		
	18	0	5	0		
	19	0	5	0	0,83	
Total 402			75	64		0,85
403	01	2	3	6		
	02	2	3	6		
	03	4	4	16		
	04	3	1	3		
	05	2	4	8		
	06	3	2	6		
	07	3	3	9	2,70	
Total 403			20	54		2,70
501	01	2	2	4		
	02	2	3	6		
	03	2	4	8		
	04	3	4	12		
	05	2	2	4	2,27	
Total 501			15	34		2,27
502	01	2	5	10		
	02	2	5	10	2,00	
Total 502			10	20		2,00
503	01	3	25	75		
	02	2	25	50		
	03	3	15	45		
	04	1	5	5		
	05	1	10	10		
	06	1	5	5		
	07	2	8	16		
	08	2	5	10		
	09	2	22	44		
	10	2	5	10		
	11	2	10	20	2,15	
Total 503			135	290		2,15
504	01	2	7	14		
	02	2	3	6		
	03	1	5	5		
	04	2	2	4		
	05	2	5	10		
	06	2	5	10		
	07	1	1	1		
	08	2	1	2		
	09	2	5	10		
	10	2	6	12		
	11	2	2	4	1,86	
	12	1	2	2		
	13	2	5	10		
	14	1	5	5		
	15	1	4	4		
	16	4	2	8		
	17	3	4	12		
	18	3	3	9		
	19	3	3	9		
	20	3	8	24		
	21	2	2	4	2,29	
	22	2	10	20		
	23	2	8	16		
	24	2	8	16		
	25	3	8	24		
	26	2	7	14		
	27	2	6	12		
	28	2	3	6		
	29	3	5	15	2,24	
Total 504			135	288		2,13

505	01	2	2	4		
	02	3	2	6		
	03	3	2	6		
	04	2	4	8		
	05	2	3	6		
	06	2	2	4	2,27	
Total 505			15	34		2,27
601	01	3	4	12		
	02	2	1	2	2,80	
	03	2	5	10		
	04	2	5	10		
	05	2	5	10		
	06	2	5	10	2,00	
Total 601			25	54		2,16
602	01	2	9	18		
	02	2	5	10		
	03	2	9	18		
	04	1	4	4		
	05	2	4	8		
	06	2	4	8	1,89	
Total 602			35	66		1,89
603	01	1	10	10		
	02	1	10	10		
	03	2	10	20	1,33	
	04	2	5	10		
	05	2	5	10		
	06	1	5	5		
	07	2	5	10	1,75	
Total 603			50	75		1,50
604	01	2	5	10		
	02	2	5	10		
	03	2	5	10		
	04	2	5	10		
	05	2	5	10		
	06	2	5	10		
	07	2	5	10		
	08	2	5	10		
	09	2	5	10	2,00	
Total 604			45	90		2,00

Total	1000	1831
Total pondéré		1,83

Annexe E

Évaluation des risques selon la méthode Delphi

Évaluation de l'importance des risques

Risques matériels	Risques matériels	Risque 1	44									
Vol sabotage	6	Vol sabotage	Risque 2	31								
Pannes et dysfonctionnements	6	4	Pannes dysfonc.	Risque 3	25							
	2											
Erreurs de saisie	6	5	6	Erreurs de saisie	Risque 4	10						
	1											
Erreurs d'exploitation	5	5	2	1	Erreurs d'exploi.	Risque 5	21					
	1	1	4	5								
Erreurs de conception	3	3	1			Erreurs concept.	Risque 6	43				
	3	3	5	6	6							
Fraude et sabotage	3					4	Fraude sabotage	Risque 7	45			
	3	6	6	6	6	2						
Indiscrétion et détournement	4	2	3		1	4	4	Indisc. détour.	Risque 8	35		
	2	4	3	6	5	2	2					
Détournement de logiciel	6	6	6	6	6	6	6	6	Détour. logiciel	Risque 9	0	
Grève et départ de personnel	5	6	5	2	3	6	6	5		Grève départ	Risque 10	16
	1		1	4	3			1	6			

Évaluation de la probabilité d'occurrence des risques

Risques matériels	Risques matériels	Risque 1	29									
Vol sabotage	4	Vol sabotage	Risque 2	18								
	2											
Pannes et dysfonctionnements			Pannes dysfonc.	Risque 3	50							
	6	6										
Erreurs de saisie			6	Erreurs de saisie	Risque 4	42						
	6	6										
Erreurs d'exploitation	4		6	6	Erreurs d'exploi.	Risque 5	29					
	2	6										
Erreurs de conception	3	2	5	5	3	Erreurs concept.	Risque 6	25				
	3	4	1	1	3							
Fraude et sabotage			3	1			Fraude sabotage	Risque 7	49			
	6	6	3	5	6	6						
Indiscrétion et détournement	6	4	6	6	6	5	6	Indisc. détour.	Risque 8	5		
		2				1						
Détournement de logiciel	6	6	6	6	6	6	6	2	Détour. logiciel	Risque 9	4	
								4				
Grève et départ de personnel	6	4	6	6	6	6	6	6	6	Grève départ	Risque 10	14
		2										

	Importance	*Valeur relative*
01	Risques matériels	44
02	Vol sabotage	31
03	Pannes et dysfonctionnement	25
04	Erreurs de saisie	10
05	Erreurs d'exploitation	21
06	Erreurs de conception	43
07	Fraude et sabotage	45
08	Indiscrétion et détournement	35
09	Détournement de logiciel	0
10	Grève et départ de personnel	16

	Probabilité d'occurrence	*Valeur relative*
01	Risques matériels	29
02	Vol sabotage	18
03	Pannes et dysfonctionnement	50
04	Erreurs de saisie	42
05	Erreurs d'exploitation	29
06	Erreurs de conception	25
07	Fraude et sabotage	49
08	Indiscrétion et détournement	5
09	Détournement de logiciel	4
10	Grève et départ de personnel	14

	Risques	*Notation*	*Importance*	*Occurrence*	*Total*
01	Risques matériels	1,64	44	29	73
02	Vol sabotage	1,77	31	18	49
03	Pannes et dysfonctionnement	1,91	25	50	75
04	Erreurs de saisie	1,68	10	42	52
05	Erreurs d'exploitation	1,92	21	29	50
06	Erreurs de conception	1,81	43	25	68
07	Fraude et sabotage	1,74	45	49	94
08	Indiscrétion et détournement	1,70	35	5	40
09	Détournement de logiciel	1,77	0	4	4
10	Grève et départ de personnel	1,67	16	14	30
			270	265	535

	Risques	*Notation*	*Total*
07	Fraude et sabotage	1,74	94
03	Pannes et dysfonctionnement	1,91	75
01	Risques matériels	1,64	73
06	Erreurs de conception	1,81	68
04	Erreurs de saisie	1,68	52
05	Erreurs d'exploitation	1,92	50
02	Vol et sabotage	1,77	49
08	Indiscrétion et détournement	1,70	40
10	Grève et départ de personnel	1,67	30
09	Détournement de logiciel	1,77	4

DELPHI
Méthode d'évaluation des risques

Dans le cadre de l'élaboration du *Plan de sécurité* il est requis d'évaluer **l'importance** de même que la **probabilité d'occurrence** de 10 risques préétablis et reconnus en matière de protection de l'information.

Le but de cette analyse est de prioriser les risques, lesquels si concrétisés, auraient un impact important sur la rencontre de la mission de l'organisation.

Les dix risques à l'étude sont :

Accidents

Risques matériels : destruction partielle ou totale des matériels ou des supports informatiques et de leur environnement.

Vol, sabotage matériel : vol de petits matériels, supports informatiques et biens divers; sabotage physique.

Pannes et dysfonctionnements : arrêts ou baisses de service d'un centre informatique.

Erreurs

Erreurs de saisie, transmission : pertes de temps, reprises, erreurs de lecture etc.; aiguillage, erreurs, parasites.

Erreurs d'exploitation : oubli ou écrasement d'un fichier ou d'une sauvegarde.

Erreurs de conception, réalisation : non conformité des traitements; non respect des délais de livraison.

Fraude, sabotage immatériel : piratage, détournement d'avantages et ou de biens; bombes logiques, virus.

Malveillance

Indiscrétion : divulgation d'informations confidentielles, détournement: non respect déontologique.

Détournement de logiciel : copie illicite, plagiat.

Grève, départ de personnes : indisponibilité du personnel.

L'objectif de l'exercice est de comparer les risques les uns avec les autres. Cette approche s'appuie sur la méthode Delphi de la Rand Corporation. On retrouve en annexe un exemple d'évaluation.

Mode d'emploi

Si cette évaluation est réalisée *individuellement* et que vous croyez, par exemple, que l'impact d'un *risque matériel* sur la mission de l'organisation est plus important que *le vol et le sabotage*, vous inscrivez le chiffre 1 dans la partie droite de la première colonne et 0 dans la partie gauche. Si par contre vous croyez que c'est le *vol et le sabotage* qui aurait un impact plus important, vous inscrivez le chiffre 1 dans la partie gauche et 0 dans la droite. Vous procédez ainsi de suite jusqu'à la fin du tableau.

Chaque participant possède un vote. Si vous faites l'exercice en groupe vous devrez répartir le total des votes dans les cases appropriées.

Tableaux d'évaluation

Le tableau qui suit vous servira d'outil pour enregistrer votre évaluation des risques pour ce qui concerne **l'importance** (impact de la concrétisation d'un risque par rapport à un autre).

Risques Matériels	Risques Matériels									
Vol Sabotage		Vol Sabotage								
Pannes Dysfonc.			Pannes Dysfonc.							
Erreurs Saisie				Erreurs Saisie						
Erreurs Exploit.					Erreurs Exploit.					
Erreurs Concept.						Erreurs Concept.				
Fraude Sabotage							Fraude Sabotage			
Indiscrét. Détour.								Indiscrét. Détour.		
Détour. logiciel									Détour. logiciel	
Grève Départ										Grève Départ

Tableau 1 : Évaluation de l'importance des risques

Le tableau qui suit vous servira d'outil pour enregistrer votre évaluation des risques pour ce qui concerne **la probabilité d'occurrence** (probabilité qu'un risque se concrétise par rapport à un autre).

Risques Matériels	Risques Matériels									
Vol Sabotage		Vol Sabotage								
Pannes Dysfonc.			Pannes Dysfonc.							
Erreurs Saisie				Erreurs Saisie						
Erreurs Exploit.					Erreurs Exploit.					
Erreurs Concept.						Erreurs Concept.				
Fraude Sabotage							Fraude Sabotage			
Indiscrét. Détour.								Indiscrét. Détour.		
Détour. logiciel									Détour. logiciel	
Grève Départ										Grève Départ

Tableau 2 : Évaluation de la probabilité d'occurrence des risques

L'analyse est habituellement réalisée par plusieurs intervenants. La compilation des résultats de l'analyse est consignée au rapport sur la Définition des besoins et ensuite présentée pour validation au Comité de sécurité. C'est à partir de cette information ainsi que celle obtenue lors de l'analyse de la situation actuelle (analyse des forces et faiblesses) que sont formulées les orientations de l'organisation en matière de protection des actifs informationnels. De ces orientations découleront des mesures à mettre en place pour corriger, s'il y a, les lacunes identifiées.

Annexe F

Détail des mesures correctives par ordre chronologique des facteurs

---

Facteur 101 : L'organisation générale – 1,30

- Thème:(01) - Définition des responsabilités – 1,47

1. Il est requis de produire un organigramme et des descriptions de fonctions définissant les responsabilités du personnel de l'organisation.

2. Les définitions des responsabilités doivent être de nature à éviter des cumuls de tâches incompatibles entre elles au point de vue de la sécurité.

3. On doit nommer un responsable de la sécurité générale (au moins pour : bâtiments, environnement, accès).

4. Un responsable au niveau de l'organisation du parc des micro-ordinateurs doit être nommément désigné (postes de travail connectés ou pas, LAN (micro-réseau), pont, passerelles).

5. Une sensibilisation régulière des décideurs et une formation adéquate des principaux acteurs, concernant les risques et la sécurité informatiques doivent être réalisées.

6. Il doit y avoir, au moins une fois par an, une réunion des responsables de l'organisation consacrée aux problèmes de sécurité générale dont les travaux sont fondés sur une étude de la vulnérabilité de l'organisation face aux différents types de risques non physiques (fraudes, détournements ou perte d'informations vitales, erreurs humaines graves, accidents sociaux, accidents économiques) au cours des trois dernières années.

7. Des contrats d'assurances doivent couvrir spécifiquement les risques informatiques (dommages matériels, reconstitution d'information, frais supplémentaires, pertes d'exploitation, détournement, responsabilité civile, etc.).

- Thème:(02) - Organisation de la sécurité – 1,15

8. Un responsable de la sécurité des systèmes d'information (RSIN) et de communication doit être nommé. Il doit pouvoir compter sur des intervenants opérationnels (STMU) prenant en charge l'ensemble des questions sécurité dès la conception des systèmes.

NB. *Le RSIN définit la stratégie de l'éducation, de l'organisation, les règles et procédures adaptées aux intervenants locaux, veille à leur mise en place et à leur exploitation avec les employés concernés.*

9 Des administrateurs(trices)-réseau compétents, bien formés, ayant clairement en charge la mission de sécurité sont requis :

- Conseil/contrôle des utilisateurs, choix des matériels et logiciels en vue de la cohérence, correspondance avec le SI central, centralisation / normalisation / contrôle / diffusion des logiciels et progiciels etc.
- Installation, adaptation, utilisation, éducation / fonctions sécurité du système, produits de sécurité, procédures de sécurité.
- Secours et centralisation de la sauvegarde.
- Gestion des droits d'accès.
- Gestion des fonctions de "tierce parties".
- Assistance de premier niveau.
- Gestion de la maintenance.

10. Il est requis de procéder à une classification des informations et des traitements par degré stratégique (prenant en compte les objectifs de disponibilité, intégrité, confidentialité du système d'information de l'organisation, englobant ce qui est supporté par PC, postes de travail/LAN.

11. Un schéma de circulation des informations, précis exhaustif, clair et mis à jour périodiquement (schéma des circuits d'informations, selon leur support entre les différents services, précisant notamment les traitements et interfaces avec l'informatique centrale et l'informatique distribuée) doit être réalisé.

12. Des procédures doivent être formalisées concernant la sécurité micro-informatique distribuées aux utilisateurs (code de bonne conduite, règles de confidentialité, contrôle de validité de certaines données, duplicata, sauvegarde des documents stratégiques, etc.).

13. Une personne compétente au plan juridique pour les questions concernant les micro-ordinateurs (contrats fournisseurs, éditeurs, maintenance, tiers, obligations CAI doit être désignée.

14. Un masque de mise en garde rappelant les sanctions prévues par les règlements et législations en cas d'accès non autorisés doit être affiché lors de la connexion, avant le *log on*.

Facteur 102: Les procédures de sécurité –1,67

- Thème:(01) – Procédures –1,73

1. Les procédures doivent être mises à jour périodiquement et appliquées systématiquement en ce qui concerne les contrôles à la réception, à la saisie, au traitement, à la transmission et à l'archivage des informations (notamment pour les traitements micro-informatiques).

2. Un responsable local doit procéder périodiquement à des contrôles (dans le cadre de procédures formelles) des informations et des traitements en amont et en aval du système informatique et, d'une façon générale, s'assurer du respect et du bon fonctionnement des diverses procédures de contrôles permanents.

- Thème:(02) - Structure des responsabilités – 1,63

3. Les contrôles doivent être proportionnés à la classification des données et opérés par des personnes responsables habilitées (en s'efforçant de séparer les tâches).

4. Chaque fonction stratégique doit avoir une personne nommément désignée pouvant jouer le rôle de correspondant informatique et de « détenteur des informations » chargé de la classification des informations ainsi que de la définition des règles et autorisations d'utilisation de ces informations (droits et privilèges d'accès, profils groupes et utilisateurs), spécifications de sauvegarde, archivage, transfert, etc.

5. Les responsabilités des créateurs et utilisateurs de programmes doivent être clairement définies et, en particulier, inclure la notion d'administrateur de programmes (responsables des programmes, des conditions d'acceptation et des sauvegardes, procédures de copie et de transfert etc.) qui peut éventuellement être requise de l'administrateur(trice)-réseau.

6. Les applications sources et objets résidant sur les postes de travail doivent toutes être identifiées (auteur et responsable connus, fonctions, etc.) par l'administrateur(trice)-réseau.

7. L'autorisation des deux administrateurs(trices)-réseau doit être indispensable pour certaines opérations critiques (modification des droits d'accès, modifications de fonctionnalités sécurité, modifications du système, etc.).

Facteur 103: La réglementation - 1,20

- Thème:(01) - Règles de contrôle – 1,31

1. On doit mettre en place une procédure de signature hiérarchisée selon le type de document traité pratiquement applicable et appliquée (en regard des responsabilités et emploi du temps des signataires d'une part, et des charges de documents à signer d'autre part).

2. On doit établir des règles écrites de sécurité et confidentialité concernant les documents et supports (disquettes) stratégiques situés dans les bureaux.

3. Les contrôles et audits réguliers et impromptus opérés par des personnes spécialisées (internes ou externes à l'organisation) doivent comprendre l'ensemble de la sécurité du système d'information.

- Thème:(02) - Gestion des pièces justificatives - 1,00

4. Dans les circuits d'informations où certains traitements sont réalisés sur les micro-ordinateurs, toute pièce administrative ou comptable doit être « marquée » (initiales et/ou signatures identifiables) par les personnes qui la traitent et les doubles des pièces administratives ou comptables doivent être annulés dès réception pour éviter des duplications d'enregistrements sur les postes de travail.

5. On doit prendre en compte la possibilité de destruction totale d'informations stratégiques (fichiers, programmes, procédures d'exploitation, documentation, etc.) sur support informatique (accident, erreur ou malveillance de type sabotage immatériel) et on doit déduire des procédures systématique de rétention des documents de base à des fins de reconstitution. Ceci entraînera chez l'utilisateur, un archivage et un classement fiables des principaux documents justificatifs originaux qui permettent, le cas échéant, une reconstitution ou une utilisation rapide de l'information sur poste de travail.

Facteur 201: Les facteurs socio-économiques – 2,00

- Thème:(01) - Les facteurs socio-économiques –2,00

1. On doit s'assurer du sentiment que le climat social est défavorable à des actions de malveillance.

2. Il est requis de prendre les moyens afin que le taux d'absentéisme moyen général de l'organisation reste stable ou diminue sensiblement.

3. Les plans à court terme et moyen terme (ou le budget prévisionnel) doivent prévoir un niveau moyen d'activité assurant une sécurité suffisante pour l'organisation.

Facteur 301: L'environnement de base – 1,50

- Thème:(01) - Sécurité du bâtiment et de l'environnement – 1,36

1. Les bâtiments doivent être construits en maçonnerie, en acier protégé ou en matériaux non-combustibles.

2. On doit tenir compte par la mise en œuvre de moyens de sécurité appropriés des stocks de matières inflammables à proximité.

3. On doit tenir compte par la mise en œuvre de moyens de sécurité appropriés des phénomènes électriques et électromagnétiques dus au voisinage (lignes à haute tension, radars faisceaux hertziens, émetteurs radio, etc.) ou à la foudre.

4. On doit tenir compte par la mise en œuvre de moyens de sécurité appropriés des nuisances liées à l'eau (eau pluviale, égouts de chauffage, d'extinction, fuites et ruissellements, gicleurs, etc.).

5. On doit procéder à des études, contrôlées périodiquement par un organisme spécialisé, sur la solidité du « clos » et la qualité de la protection mécanique périphérique (mur, clôture, etc.).

6. On doit procéder à une vérification périodique des installations électriques (et en particulier des défauts de neutres et de la mise à la terre des prises des postes de travail) par un service ou un organisme spécialisé entraînant un suivi des recommandations prescrites.

- Thème:(02) - Sécurité physique de base : postes de travail-LAN – 1,47

7. On doit mettre en place une conception d'ensemble du câblage, une réalisation normalisée fiable faisant en sorte que les piquages de nouveaux postes de travail-LAN et extentions se fassent sans difficulté excessive.

8. On doit disposer d'un inventaire à jour de tous les équipements (serveurs, divers, postes de travail, modems, multiplexeurs, concentrateurs, ponts, passerelles, etc.) avec leur emplacement et leurs connexions.

9. Les locaux contenant les équipements ainsi que tous les équipements (notamment têtes de ligne) doivent être isolés et protégés à raison de leur caractère stratégique (sécurité physique, accès).

10. Les points de connexion doivent être recensés, sécurisés, désactivables par le système (hors fonction) et régulièrement inspectés.

11. Les points d'entrée possibles (tableaux de connexion, *jacks*, *jumpers*, etc.) doivent être recensés, sécurisés et régulièrement inspectés.

12. Les postes de travail doivent être dépourvus de lecteurs de disquettes (ou l'accès en doit être physiquement interdit).

13. Tout équipement provenant de l'extérieur doit être inspecté et réceptionné avant sa mise en service.

14. On doit utiliser des moyens de lutte contre le rayonnement (matériel TEMPEST, blindage des câbles et équipement, faradisation de locaux) lorsque le micro-réseau-LAN véhicule des informations confidentielles critiques.

15. Le câblage doit être isolé et à accès physique contrôlé (isolation des câbles, gaines spécifiques non facilement accessibles, surveillance, etc.).

NB : *Le contrôle portera sur le répartiteur général, le répartiteur de distribution, les câbles de distribution - de rocade - et capillaires, les points d'accès et prises, les modules de raccordement. On procédera en outre régulièrement à de mesures (écho, impédance, analyse des parasites) et l'on raccordera la surveillance du réseau à un poste central.*

Facteur 302: Les contrôles d'accès physique – 1,83

- Thème:(01) - Contrôle d'accès – 2,14

1. On doit implanter un système de contrôle systématique des accès aux bâtiments (issues principales, annexes, stationnements, etc.).

2. Des procédures de contrôle des accès du personnel au locaux de l'organisation, en dehors des heures ouvrables sont nécessaires.

3. Des procédures de contrôle des accès aux bâtiments pour les intervenants extérieurs autorisés (nettoyage, dépannage, etc.) doivent être établies.

4. Le personnel contrôlant les accès doit être sensibilisé au risque de vol de petits matériels (micros, postes de travail, modems, etc.), et effectuer des contrôles physiques impromptus (sortie, stationnement, etc.) ou disposer de moyens de détection de sortie illicite de matériel.

5. On doit mettre en place des procédés anti-vol pour les petits matériels (fixations, marquage de propriété indélébile, système déclenchant l'alarme en cas de sortie, blocage électronique, etc.).

6. On doit disposer d'une procédure (gestion chronologique des sujets vis-à-vis des matériels et surtout de leur contenu : fichiers et programmes) et de moyens spéciaux pour la sortie de systèmes portables.

7. Une trace écrite identifiant chaque entrée/sortie de petit matériel doit être disponible.

8. Les serveurs doivent être sécurisés physiquement et disposés dans des pièces fermées à accès contrôlé (la console devant physiquement résider au même endroit).

- Thème:(02) – Intrusion – 1,00

9. En dehors des heures ouvrables, on doit exploiter un système cohérent et complet de détection d'intrusion protégeant les bâtiments du type : détection associée à une alarme simple; détection avec enregistrement de l'intrusion; détection associée à une téléalarme. Le système de détection d'intrusion doit avoir fait l'objet d'une réception par un organisme spécialisé.

10. Les bureaux renfermant des petits matériels et des supports informatique doivent pouvoir fermer à clé (serrure certifiée) et être effectivement être fermés à clé.

Facteur 303: La pollution – 1,60

- Thème:(01) - Poussières et inflammabilité – 1,33

1. On doit prendre les mesures de protection et d'entretien (dépoussiérage) correspondant à des risques spécifiques de pollution (personnel formé, etc.).

2. Il doit y avoir interdiction de fumer dans les bureaux contenant les postes de travail, serveurs, etc.

- Thème:(02) - Électricité statique – 2,00

3. Puisqu'il y a constat des nuisances dues à l'électricité statique, on doit installer un revêtement de sol ou un tapis anti-électricité statique sous les matériels (postes de travail, serveurs, etc.) ainsi que des parafoudres (lignes électriques et télécommunications).

Facteur 304: Les consignes de sécurité physique – 1,20

- Thème:(01) – Consignes – 1,20

1. On doit émettre des consignes générales de sécurité correctement affichées (sécurité incendie, sécurité des personnes), notamment dans les bureaux contenant des équipements.

2. Le personnel doit être informé et formé à la sécurité, notamment aux consignes, et participer régulièrement à des exercices.

3. Les bureaux contenant des postes de travail ou des serveurs, nécessitent des consignes spécifiques (débranchement ou coupure générale en cas de début d'incendie ou de court-circuit, enlèvement rapide des coffres de sauvegarde en cas d'incendie, appel à un officier de sécurité, etc.).

Facteur 305: La sécurité incendie – 1,80

- Thème:(01) - Détection automatique – 2,00

1. On doit implanter un système de détection automatique pour l'ensemble des bâtiments (installations donnant lieu à un certificat de réception par un organisme spécialisé), périodiquement entretenu.

2. Les systèmes de détection automatique doivent être reliées à un poste permanent de surveillance susceptible de déclencher une intervention rapide.

- Thème:(02) – Extinction –1,33

3. Des extincteurs mobiles doivent être installés avec agent d'extinction adapté au contenu des locaux, en nombre suffisant et correctement entretenus dans tous les bureaux contenant des petits matériels et des supports informatiques (ou à proximité immédiate).

4. Le type d'extinction (pour feu de papier, pour plastique, etc.) doit être clairement indiqué et adapté.

5. Les documents ou supports informatiques (disquettes, DON, etc.) contenant des informations stratégiques, stockés dans les bureaux doivent être entreposés dans des meubles réfractaires.

Facteur 306: La sécurité dégât des eaux – 0,80

- Thème:(01) – Prévention – 0,80

1. Les utilisateurs de micro (postes de travail, serveurs, etc.) doivent éviter d'entreposer des liquides ou de conserver des boissons à proximité des matériels.

2. On doit vérifier qu'il n'existe pas de canalisations d'eau apparentes ou traversant des espaces cachés dans les bureaux contenant du matériel informatique (on recensera les vannes d'arrêt).

Facteur 307: Fiabilité de fonctionnement matériels informatiques – 1,55

- Thème:(01) - Qualité du système – 1,60

1. Les matériels et les systèmes doivent faire l'objet d'une diffusion commerciale courante (c'est-à-dire des matériels standards connus et réputés).

NB : *L'ensemble des systèmes et logiciels doit être standard et assurer en particulier une convivialité de bon niveau.*

2. Le choix de la configuration doit reposer sur une étude comparative des caractéristiques en matière de sécurité, menée par la DTI pour des raisons de cohérence (maintenabilité, portabilité, compatibilité, évolutivité, fiabilité, contrôle d'accès).

3. On doit se prémunir d'un stock de secours des petits matériels (postes de travail/serveurs claviers, écrans, contrôleurs, modems, etc.), et une personne doit être formée à la maintenance simple d'urgence.

4. Le micro-réseau-LAN doit intégrer des dispositifs à tolérance de panne (serveurs multiples, *disk mirroring*, *canal mirroring*, etc.) fondés sur la redondance des unités stratégiques.

5. Le système (DOS, NOS, etc.) doit intégrer des mesures de prévention du type :
   - Gestion dynamique des mauvais secteurs (*hot fix*);
   - Lecture après écriture (*read after write* : RAW);
   - Redondance de l'information (IR sur répertories et FAT);
   - Suivi des transactions (TTS).

- Thème:(02) – Environnement – 1,40

6. Les conditions de température (15-30 C) et d'hygrométrie (40-60 %) dans les bureaux contenant des matériels informatiques doivent être mesurées (aux périodes défavorables) et être acceptables pour les matériels installés.

7. Il est requis de mettre en place un régime du neutre de l'immeuble approuvé par le code du bâtiment.

8. Des appareils de régulation de tension (ondulateurs ou stabilisateurs, individuels ou collectifs) pour l'alimentation des postes de travail et des serveurs sont requis.

❖ NB : *En cas de spécifications de haute disponibilité, il faut ajouter une installation autonome (batteries relais + groupe électrogène).*

Facteur 308: Les systèmes et procédures de secours – 1,73

- Thème:(01) - Moyens de secours – 1,73

1. On doit disposer d'un plan de secours différencié (sinistres locaux/sinistres globaux) et de moyens adaptés et testés pour faire face aux événements majeurs (un micro-réseau-LAN ou l'ensemble du système).

2. On doit disposer de solutions de secours pour faire face à une indisponibilité ponctuelle de postes de travail (micros en libre service, micros disponibles partiellement ou totalement dans d'autres bureaux, micros jumeaux, etc.) et de certains périphériques (imprimantes, tables traçantes, scanners, etc.).

3. On doit être en mesure de se procurer et installer dans un délai admissible (selon le caractère stratégique) des matériels de remplacement (système et connexion).

4. On doit pouvoir se procurer et installer dans un délai admissible (selon le caractère stratégique) des logiciels de remplacement (applicatifs, etc.).

5. Il doit y avoir un mode de secours en cas de sinistre affectant les liaison de communication LAN ou WAN (autres lignes, faisceaux hertziens, supports magnétiques, etc.).

Facteur 309: La cohérence des systèmes – 2,00

- Thème:(01) - Cohérence des systèmes – 2,00

1. On doit assurer la cohérence des systèmes répartis les uns par rapport aux autres (matériels, logiciels de base, langages, progiciels, réseaux, etc.) ainsi que de la cohérence et la compatibilité des systèmes répartis avec l'informatique centrale.

NB : *On disposera d'une documentation complète et à jour :*

- *Schémas LAN/postes de travail, LAN/LAN, LAN/WAN, LAN/Hôtes*
- *Distribution des systèmes et produits*
- *Définition des liaisons*

On définira et contrôlera la stratégie LAN, évolutions et extensions LAN. On suivra les nouveaux produits et services et les fournisseurs (homologation).

2. Il doit y avoir des dispositifs de contrôle efficaces pour le passage d'informations (en mode automatique) LAN/LAN, LAN/WAN, LAN/hôte.

Facteur 310: Le personnel – 1,45

- Thème:(01) - Formation du personnel – 1,45

1. Il est requis de donner une formation et une information régulières au personnel concerné par l'évolution des matériels et des systèmes.

2. On doit former le personnel sur les logiciels ou applications utilisées.

3. On doit procéder à une sensibilisation et une information de l'ensemble du personnel aux problèmes de sécurité (entraînant par exemple la définition d'un code de déontologie). En particulier, on doit concevoir un guide de sécurité micro (poste de travail/micro-réseau-LAN) clair, simple, faisant l'objet d'une diffusion et d'explications régulières, associé par exemple à des notions ou affiches (bureaux, matériels, produits, etc.).

4. Les utilisateurs doivent être bien informés des procédures, manipulations ou commandes qui peuvent être dangereuses sur un poste de travail (formatage, *delete*, etc.) et savoir à qui il faut faire appel en cas d'incident.

5. On doit mettre en place une information déontologique et juridique concernant la propriété des programmes internes et progiciels externes (droits de reproduction, risques de diffusion des virus, etc.).

6. On doit mettre en place un système d'information de sécurité à destination des utilisateurs postes de travail/micro-réseau-LAN, comprenant par exemple :

- un périodique (nouveautés, recommandations, incidents, etc.);
- une messagerie ou une "*Hot line*" pour les urgences (administrateur-réseau-LAN).

Facteur 311: Les plans informatique et de sécurité – Architecture – 1,29

- Thème:(01) - Plan et procédures informatique et sécurité – 1,83

1. Le plan de sécurité des systèmes d'information doit couvrir le domaine des micros (*stand alone* fixes et portables) et des LAN (serveurs, postes de travail, etc.) : analyse des vulnérabilités et des menaces, solutions, organisation de la sécurité.

2. La DTI doit travailler systématiquement dans le cadre d'un plan qualité, incluant un système d'assurance qualité fondé sur des contrats clients-fournisseurs formalisés, en conservant un rôle exclusif de maître-d'œuvre, et en assurant les responsabilités qui en découlent.

NB : *On établira par exemple, des contrats de services pour l'administration du réseau.*

3. La direction informatique doit définir une répartition des rôles cohérente et efficace (notamment du point de vue de la sécurité) entre les différents acteurs de l'informatique et les utilisateurs en matière :

- de définition du LAN et de ses attachements;
- de choix de progiciels utilitaires et de gestion;
- d'installation des matériels et logiciels (environnement, câblage, connexion, gestion des versions de logiciels/postes de travail ou serveurs, maintenance);
- de documentation descriptive LAN;
- de réalisation des sauvegardes;
- d'analyse du réseau à partir d'outils PC;

- Thème:(02) – Architecture – 1,00

4. Il est requis de réaliser une étude d'optimisation de la topologie WAN/LAN (partitions/concentrateurs/distribution postes de travail : recherche de l'ASM (arbre sous-tendant minimum) pour le réseau de bas niveau (méthodes de Kruskal, Prim, ADD, DROP).

NB : *Cette étude doit intégrer la prise en compte utilisateurs/postes de travail, les interconnexions de serveurs, le partage des applications et données ainsi que des ressources catégorielles entre les utilisateurs.*

5. On doit procéder à la définition des spécifications de performance LAN/postes de travail et procéder à des projections de performance lors de l'évaluation de sélection de l'offre.

6. En cas de transmission multimédia ou en cas de besoins de haute qualité ou lorsque le domaine géographique est étendu ou perturbé (haut débit, haute performances), on doit utiliser un mode de transmission à large bande (câblage coaxial ou fibre optique) et prévoir un mode spécifique de maintenance des modems.

7. Les choix de supports, de topologie, de systèmes doivent être adaptés au contexte d'utilisation :

- Sauf si le LAN est peu étendu (moins de 1 000 m) et dans un contexte peu perturbé, on devrait éliminer les supports de transmission de type paire torsadée.
- Si l'on a retenu une topologie en anneau (exemple : Token Ring), on devrait limiter le nombre de nœuds actifs (plus petit que 250 sur fibre optique, et 100 sur autres supports), intégrer les risques de coupures, et prendre en compte les extensions possibles dès le départ.
- Si l'on recherche une grande disponibilité et si les noeuds sont peu éloignés, on devrait retenir une topologie en étoile (exemple : Starian, Arcnet, Novell Netware).
- Si l'on a retenu une topologie en bus (exemple : Ethernet, Arcnet, Token Bus), on devrait prendre en compte les risques de coupures et les extensions possibles (topologie arbre).

8. Pour le choix du système d'exploitation du LAN, on doit prendre en compte le type de serveur et les spécificités de base (accessibilité, exigences mémoire, fiabilité, sécurité).

9. Le système d'exploitation doit intégrer une offre de services de sécurité dans les couches OSI, au moins en A, B, E et F et à un niveau acceptable et correspondant au degré stratégique des informations traitées (TCSEC/CI).

❖ A- Authentification (e, 4, 6), B- Confidentialité séquences (1, 3, 4, 6) C- Confidentialité sans connexion (3, 4, 6), D- Confidentialité champs (6), E- Contrôle d'accès (3, 4, 6, 7), F- Intégrité séquences (3, 6), G-Intégrité champs (6), H- Non-répudiation (6), I- Secret du flux (1, 7) ?

10. Les système de transmission doit utiliser des séquences de contrôle paquet (CRC) définies à partir d'un polynôme de degré au moins 16.

Facteur 401: La sécurité logique de base – 2,34

- Thème:(01) - Identification/Authentification – 2,26

1. La définition des droits et habilitations a-t-elle été effectuée en collaboration avec les utilisateurs, fondée sur la classification des objets (données, traitements) et des sujets ?

NB : *L'administrateur(trice)-réseau doit définir les groupes d'accès (avec leur DA et privilèges) et le propriétaire fonctionnel définit avec l'administrateur(trice)-réseau les rattachements d'utilisateur aux groupes.*

2. Il est requis de mettre en place un système d'identification et d'authentification par mot de passe non évident pour chaque utilisateur (un couple identifiant-authentifiant unique par utilisateur). (Le *log-on* implique obligatoirement l'introduction par l'utilisateur du couple identifiant/authentifiant).

3. Les serveurs doivent être en mesure d'identifier, lors du *log-on*, le poste de travail et son point de connexion.

4. L'accès à des ressources critiques doit nécessiter, outre l'authentification de l'utilisateur, la vérification de validité du poste de travail et de la connexion du poste de travail demandeur.

5. Les serveurs doivent être en mesure de demander l'identification/authentification, même après le *log-on* (notamment lors de demandes d'accès aux ressources stratégiques).

6. On doit voir à ce qu'il n'y ait aucune possibilité d'identification multiple (le même utilisateur ou même l'administrateur(trice)-LAN connecté(e) sur plusieurs nœuds), ou bien si c'est possible, on devrait disposer d'un système d'alarme et de suspension automatique de session en cours.

7. Lors d'anomalies réseau, et dès lors qu'il est nécessaire de modifier les privilèges d'accès, il doit obligatoirement y avoir une ré-authentification.

8. Les *log-on* corrects doivent afficher la date et l'heure du précédent *log-on / log-off.*

9. On doit avoir la possibilité de désactiver le clavier pendant certaines tâches spécifiques.

- Thème:(02) - Contrôle d'accès – 2,39

10. Il est requis de mettre en place un système (intégré ou annexé) fiable de contrôle logique des accès informatiques (avec gestion des mots de passe, changements, enregistrement) ou avec des procédures externes (clé, carte à mémoire, reconnaissance biométrique, etc.) .

11. Les mots de passe doivent répondre aux critères élémentaires de sécurité :

- Longueur d'au moins 6 caractères.
- Nom triviaux, mixtes (alphanumériques + autres).
- Adaptés aux enjeux (notamment pour la périodicité de changement, au minimum 4 fois/an et beaucoup plus fréquemment pour les mots de passe d'accès au réseau).
- Restrictions d'usage (recyclage d'anciens mots de passe, d'identifiants, etc.).
- Non visualisables (écrans).
- Vérification lors des créations/changements (2 entrées), avec un temps maximum et un nombre d'essais maximum alloués pour l'entrée.
- Suspension des identifiants et mots de passe après une période d'arrêt du système fixée par l'administrateur(trice) du LAN.

NB : *L'administrateur(trice)-LAN et les utilisateurs(trices) doivent veiller au changement de mot de passe dès qu'ils soupçonnent une compromission.*

12. Les postes de travail doivent être dépourvus d'entrée disquette ou, à défaut, le système doit être systématiquement initialisé à partir d'un disque amovible conservé dans des conditions de haute sécurité (ou bien utilise-t-on un CD-ROM pour tous les logiciels sensibles).

13. Tous les fichiers (programmes et données), ainsi que les autres ressources (périphériques, fonctions système) doivent être protégés.

14. Le contrôle des accès aux fichiers doit être exercé aux niveaux fichiers / répertoire / sous-répertoire.

15. Les privilèges d'accès aux fichiers doivent inclure au moins « *Read* », « *Read only* », « *Write* » (avec séparation création/mise à jour), « *Execute* », « *Execute only* », « *Create* », « *Rename* », « *Delete* », « *Change access* », « *None* ».

Ces privilèges doivent être attribués (groupes/utilisateurs) par l'administrateur(trice) de LAN, avec les propriétaires fonctionnels, en se fondant sur le droit et le besoin d'en connaître. On restreindra donc au maximum les droits (*Read only*, *Execute only*, au moins pour les fichiers sensibles .COM et .EXE).

16. L'accès aux ressources doit être assignable sur une base individuelle / groupe / public (les rattachements utilisateurs/groupes doivent être uniques de préférence), et intégrer la sélectivité (par poste de travail, par connexion, par plage de date-heure etc.).

17. Un système intégré et fiable de contrôle logique des accès pour toutes les applications stratégiques avec gestion des mots de passe, changements, enregistrements et/ou avec des procédés externes, clés, carte à mémoire est requis.

18. On doit mettre en place une procédure complémentaire d'accès par mot de passe pour l'accès aux fichiers stratégiques.

19. En plus des mots de passe associés aux privilèges superviseurs, chaque administrateur(trice) de LAN doit disposer de mots de passe pour l'utilisation normale du système.

20. Les sessions des postes de travail doivent être systématiquement suspendues après une période d'activité déterminée par l'administrateur(trice) du LAN et automatiquement fermées après une période déterminée.

21. Après une alarme pour *log-on* infructueux, on doit pouvoir générer une simulation de *log-on* et de session (afin de conserver la connexion pour analyse et pour action).

22. On doit vérifier qu'il n'y ait aucune possibilité d'accès au serveur après un *boot* sur poste de travail.

23. Une procédure de sécurité est nécessaire assurant la cohérence du contrôle d'accès lorsque plusieurs sous-systèmes, ayant leurs propres procédures de droits d'accès, sont en demande d'accession parallèle ou séquentielle, notamment lorsque plusieurs serveurs coopèrent et se passent la main (définition du serveur superviseur gérant les délégations et circulations des droits en jeton et gérant les échanges inter-serveurs nécessaires pour définir un droit d'accès de session).

Facteur 402: La sécurité des télécommunications – 0,85

- Thème:(01) - Sécurité générale WAN/LAN

1. L'accès aux fonctions de communication doit être restreint (utilisation, programmes, données, transactions, calendrier, chronologie, procédures, etc., spécifiques de contrôle d'accès identification/authentification), ces accès devant être enregistrés (*log*).

2. Tous les messages de communication doivent être authentifiés (MAC, signature, etc.).

3. Les communications stratégiques doivent être chiffrées (algorithme certifié, procédure automatique, procédure de chiffrement de tout en bout ou par lien).

4. Les transactions stratégiques ne doivent être effectuées qu'à partir de matériels placés dans des locaux à accès contrôlé et/ou disposant d'un système spécifique de sécurité d'accès logique (lecteur de carte à mémoire par exemple).

5. On doit implanter des procédures particulières de connexion pour les postes reliés au réseau commuté.

6 Les numéros passés par le RTC via l'autocommutateur doivent être contrôlés.

7. On doit procéder à un contrôle de la ligne appelante (exemple : Datapac) et à un contrôle de l'appelant lorsque c'est possible (exemple : Numeris).

8. On doit procéder à la fermeture des éléments du réseau en dehors des heures de sessions.

9. On doit mettre en place des procédures afin d'éviter le rejeu (séquencement, chronodatage).

10. On doit utiliser des générateurs de bruit blanc pour les transactions confidentielles lors de leur déclenchement sur le réseau.

11. Il est requis de mettre en place des procédures de non-répudiation (émission notamment et réception accessoirement) lorsque cela est nécessaire.

12. Lors de transmissions stratégiques, le protocole de connexion doit permettre de vérifier l'authenticité des entités (demande de liaison au serveur, vérification et distribution de la clé de session et *timing* par le serveur, envoi de l'émetteur au récepteur d'un message d'ouverture.

- Thème:(02) - Sécurité spécifique LAN

13. Toutes les fonctions d'exploitation du réseau (protocole local et protocoles d'exploitation du réseau|protocole local et protocoles d'interfaces) devraient être gérées uniquement sur la console d'un serveur dédié, par le ou la seul(e) administrateur(trice)-LAN.

14. Toutes les communications, sans exception, doivent passer par un serveur.

15. On doit s'assurer qu'il n'y ait aucun usage non autorisé ou non contrôlé de moniteurs de trafic, routeurs, etc.

16. On doit faire des tests (par réflectomètre) pour détecter d'éventuelles prises pirates.

17. Le LAN doit procéder à un contrôle de l'appelant (*call back*).

18. L' information stratégique envoyée sur le LAN, doit être chiffrée.

19. On doit procéder à des essais de pénétration WAN et surtout LAN (éventuellement via WAN).

Facteur 403: La protection et le contrôle des données – 2,70

- Thème:(01) - Protection des données – 2,70

1. L'organisation et la structure des données doit tenir compte des contraintes de sécurité :
   - Fichiers/répertoires/sous-répertoires (en liaison avec les droits et privilèges d'accès et de chiffrement, contraintes de périodicité de sauvegarde);
   - Structure des clés et enregistrements (accès au champ, intégrité du champ);
   - Zones de contrôle et de redondance (intégrité des séquences).

2. L'intégrité des données doit être assurée pour les données partagées (fichiers, BD) par des dispositifs spéciaux (verrouillage temporaire et gestion des accès concurrents).

3. Les utilisateurs doivent disposer systématiquement de répertoires privées pour stocker leurs fichiers privés.

4. On doit posséder un système automatique de contrôle d'intégrité des fichiers (avec alarme de l'administrateur(trice)-LAN).

5. Les données confidentielles stockées doivent être chiffrées (ceci inclut les fichiers de mots de passe, de pointeurs et de clés, d'audit, etc.), les procédés et algorithmes de chiffrement doivent être certifiés et automatisés : les textes en clair doivent être automatiquement physiquement effacés après chiffrement.

6. On doit utiliser des procédures spéciales de protection des fichiers au sein du système d'exploitation (exemple : procédure *hidden*).

7. On doit utiliser des procédures de protection, si elles existent, dans les logiciels de base et dans les logiciels de gestion des données :
   - au niveau applicatif (par défaut par rapport au système d'exploitation);
   - au niveau fichiers (chiffrement, droits et privilèges d'accès);
   - au niveau du champ (privilèges d'accès), exemple : cellule protégée/tableurs.

Facteur 501: L'archivage / désarchivage – 2,27

- Thème:(01) - Procédures et gestion des supports – 2,27

1. On doit mettre en place des procédures et des matériels de destruction des documents confidentiels adaptés aux supports (papier, supports magnétiques, microfiches) dès qu'on n'a plus l'usage de ces documents.

2. On doit mettre en place des procédures d'identification des supports (archives, sauvegardes, divers) qui permettent un classement fiable, une reprise rapide, un risque d'erreur de manipulation minime, et surtout qui garantissent la confidentialité).

3. Il est requis d'utiliser des locaux et/ou armoires et/ou coffrets de sécurité permettant de stocker les disquettes micro dans des conditions de sécurité acceptables.

4. Les disquettes originales de progiciels (ainsi que les contrats de licence) doivent être stockées dans une armoire de sécurité.

5. On disposera de procédures et de supports d'archivage fiables en regard de la durée de conservation de l'information souhaitée.

Facteur 502: La saisie et le transfert classique des données – 2,00

- Thème:(01) - Transfert sécurisé des données – 2,00

1. Lors de transferts de supports magnétiques contenant des données stratégiques, on doit utiliser des conteneurs sécurisés (fermés à clés, protégés contre l'effacement, les chocs, etc.) des convoyeurs accrédités (de préférence externes à l'organisation) avec une procédure de contrôle d'acheminement (bordereau horodaté avec accusé de réception) ou bien on doit utiliser du télé transfert (avec acquittement et signature numérique).

2. On doit avoir des règles particulières pour les progiciels et informations sur micros portables (et éventuellement connectables) hors de l'organisation (interdiction de sortie de certaines données ou progiciels et/ou chiffrement en cas de sortie, et/ou modification temporaire des droits et privilèges d'accès et/ou procédure préalable de test/sauvegarde suivie d'une procédure de test/réception au retour).

Facteur 503: La sauvegarde – 2,15

- Thème:(01) – Sauvegarde – 2,15

1. Il faut au moins une sauvegarde systématique (périodicité adaptée à une reconstitution raisonnable) de l'ensemble des informations (données, programmes, procédures, etc.).

2. Ces sauvegardes doivent être à deux niveaux : 1er niveau (fréquence élevée) stockées sur place et 2e niveau (fréquence raisonnable) stockées dans des locaux de sauvegarde éloignées du bâtiment considéré et correctement protégés (vol, vandalisme, intrusion, incendie, hygrométrie, température, corrosion, etc.), sachant que les supports de sauvegarde doivent faire l'objet de procédures spécifiques de transport sécurisé.

3. La sauvegarde doit être réalisée en utilisant des systèmes adéquats (*streamers*, DON/WORM-WMRM ou DAT plutôt que disquettes, cartouches ou bandes) et les fonctionnalités du DOS (complète/archive / incrémentale/incrémentale séparée/différentielle, selon qu'il s'agit de sauvegardes d'exploitation ou de recours), en veillant au respect des règles de sécurité pendant la sauvegarde (initialisée sur un serveur superviseur, un serveur de sauvegarde ou un poste de trqavail. Dans ce dernier cas, on veillera à sécuriser le profil spécial de l'utilisateur de sauvegarde) et en assurant la cohérence des sauvegardes centrales et locales.

4. Il doit exister pour chacun des fichiers (ou pour l'ensemble) des règles strictes mentionnant le nombre de générations, la périodicité, le lieu et la durée de stockage des sauvegardes, ainsi que des procédures (techniques, utilisateurs) de reprise précisant notamment la conduite à tenir.

5. On doit procéder périodiquement à des tests de restauration des sauvegardes (vérification de l'intégration du contenu).

6. On doit posséder une sauvegarde de la documentation (système d'exploitation, progiciels, logiciels, etc.) dans des locaux externes à l'organisation correctement protégés.

7. Entre deux sauvegardes, on doit mettre en place des procédures informatisées (journalisation) ou non (conservation des documents) permettant de reconstituer facilement les données.

8. Il doit exister des moyens régulièrement mis en œuvre de contrôle de l'application des règles et procédures (en pratiquant notamment des audits et inventaires des supports de sauvegarde).

9. Un système centralisé (serveur dédié) de sauvegarde est requis pour réaliser automatiquement les sauvegardes avec les caractéristiques définies, ou, à défaut, il doit exister un service chargé d'organiser et contrôler les sauvegardes (installation de procédures, ramassage systématique des disquettes de sauvegardes, etc.).

10. La maîtrise de l'évolutivité des facteurs de sauvegarde (versions de système d'exploitation ou de paramétrage, versions de supports, etc.) est nécessaire.

11. On doit établir des procédures de sauvegarde « très haute sécurité » pour les informations stratégiques (demande élevée d'intégrité) reposant sur une procédure de certification-scellement (MAC).

Facteur 504: La sécurité de l'exploitation – 2,13

- Thème:(01) -Sécurité générale de l'exploitation – 1,86

1. La gestion du réseau doit être organisée selon les recommandations ISO (fonctionnelles et temporelles) :
   - Gestion des anomalies;
   - Gestion comptable;
   - Gestion de la configuration;
   - Gestion des performances;
   - Gestion de la sécurité.

NB : *Les principales catégories d'outils standard sont les analyseurs (réseau, audit-trail, métrologiques, surveillance), les administrateurs, les intégrateurs (réseaux hétérogènes notamment).*

2. Les micro-ordinateurs ou postes de travail devraient être mono-utilisateurs.

3. On doit utiliser des procédures automatisées (cataloguées) d'exploitation à chaque fois que c'est possible et parmi elles, on doit prévoir celle de « gestion des résidus » (effacement physique des zones mémoires contenant des données contenant des données sensibles).

4. Une documentation complète est requise par matériel et logiciel de base et doit être stockée dans un lieu protégé.

5. Une documentation complète est requise par application et doit être stockée dans un lieu protégé.

6. On doit posséder une procédure sécuritaire d'organisation des fichiers et des répertoires (en particulier séparation données/traitements).

7. On doit définir des règles d'identification et de gestion des supports magnétiques.

8. Les règles d'identification des fichiers doivent être facilement reconstituables.

9. On doit avoir des règles précises et limitatives pour l'utilisation de commandes et outils dangereux par des utilisateurs (exemple : formatage ou effacement physique des supports ou encore PC-Tools, Norton, etc.).

10. Des règles de journalisation systématiques et sécuritaires (procédures d'enregistrement, de protection, analyse, règles d'accès, supports ineffaçables, etc.) doivent être définies. Le contrôle de la journalisation doit être centralisé.

11. On doit prévoir des procédures ad hoc de contrôle d'accès aux ressources qui évitent un contournement des droits (par exemple : copie autorisée par usage illicite), soit en réglant les paramètres du système d'accès, notamment la granularité des privilèges au niveau fichiers/répertoires/sous répertoires, soit par d'autres procédures (interdiction physique de copie, chiffrement, etc.).

- Thème:(02) - Sécurité spécifique d'exploitation LAN – 2,29

12. Il doit y avoir un lancement systématique d'une session spéciale (nettoyage mémoires) après chaque déconnexion due à une station de travail (*log-off*) au serveur (exemple : suite à inactivité) ou accidentelle (même temporaire comme pour les cas d'indisponibilité du réseau).

13. Toutes les fonctions de sécurité, et toutes les modifications du système, doivent être systématiquement réalisées qu'à partir de la console et seulement par l'administrateur(trice) LAN.

14. Aucun serveur ne doit être contrôlé à distance (par exemple, à partir d'un poste de travail) et aucun serveur ne doit être en mesure d'exécuter des travaux lancés à distance (postes de travail, ponts, passerelles, routeurs, convertisseurs de protocoles, PADS, connexions à hôte *main frame*).

15. Le *log-on* du superviseur doit être réalisé qu'à partir de la console.

16. Il ne doit pas y avoir de programme utilisateur exécuté sur les serveurs (à partir d'une installation par une station de travail et il doit être impossible d'ajouter sans contrôle des programmes exécutables dans les ressources communes (idem pour macro-instructions et macro-librairies).

17. Les privilèges des programmes doivent être « *Read only* » ou « *Execute only* » (selon le niveau de sécurité requis, l'utilisateur, la licence d'utilisation de logiciel, etc.) sur des répertoires de même privilège (idem pour les macro-librairies).

NB : S'il y a des fichiers « overlay » attribution du privilège Write/Modify mais les fichiers .EXE et .COM doivent résider sur des sous-répertoires « Read only ».

18. L'administrateur(trice) de LAN doit contrôler régulièrement les délégations « parentales » de droits et privilèges d'accès en nature et par niveau (répertoire, sous répertoire/fichier).

19. L'administrateur(trice) du LAN doit tenir à jour un inventaire des logiciels et progiciels (contrôle des licences d'utilisation) utilisés sur les serveurs et postes de travail.

20. On doit conserver (sous forme chiffrée) et analyser les journaux (*logs*) qui reprendront notamment les postes suivants : essais infructueux de *log-on*; essais d'opérations non autorisés; suspensions, arrêts délibérés et accidentels; changement dans les fonctions sécurité, changement des paramètres système ou du système; *log-on/log-off*; accès aux ressources stratégiques. (Le *log* enregistrera au moins : ressource/opération/utilisateur/date-heure/et si possible poste de travail/point de connexion).

21. Outre l'analyse ordinaire des *logs*, on doit disposer d'un système d'analyse permanent déclenchant une alarme lors du dépassement de seuils fixés sur les postes cités (le système doit disposer de fonctions permettant facilement d'exploiter les *logs* et de disposer des droits d'accès).

- Thème:(03) - Sécurité virus – 2,24

22. Les utilisateurs doivent être informés des symptômes des virus informatiques et en déduire des prescriptions de détection (rapidité d'exécution, usage disque, erreurs non usuelles; répertoires; modification de taille des programmes et fichiers, dates de mise à jour; noms des programmes et fichiers; charge réseau, etc.).

23. Après une alerte de détection au virus, il doivent savoir ce qu'il faut faire et le faire : les recherches et les premières mesures d'urgence (isolement du système infecté, analyse fine, détermination de l'auteur et du mode de propagation, restrictions réseau, appel à l'aide sur le réseau, avertissement de ceux qui risquent d'avoir été contaminés).

24. On doit savoir ce qu'il faut faire pour décontaminer un micro et le faire le cas échéant (reformatage disque dur, rechargement du système original, des applications et des fichiers, etc.).

25. On doit utiliser des moyens logiciels reconnus efficaces en prévention et/ou détection des virus.

NB : *Disposant de fonctions efficaces (Scanning, integrity checking CRC, Adv. checking, Behaviour, Réduction of false alarms, Repair, Hard schell, etc.), avec une cotation au moins égale à 7.4 (classement NSTL/Datapro).*

26. Il doit y avoir des règles de contrôle et de restriction d'accès pour le passage d'informations (support magnétique ou réseau) d'un matériel à l'autre.

27. On doit utiliser systématiquement à chaque fois que cela est possible, la protection « *Ready only* » l'interdiction d'écriture physique (à ne pas confondre avec l'écriture optique).

28. On doit prévoir des procédures systématiques et efficaces de non-dispersion d'un virus par LAN/WAN après détection (et d'information des acteurs tiers susceptibles d'être concernés).

29. On doit charger sur les stations de travail (si c'est autorisé) ou sur les serveurs (directement ou en téléchargement) que des fichiers (données et programmes) ayant fait l'objet d'un contrôle préalable (quarantaine, analyse par logiciel, etc.).

Facteur 505: La maintenance – 2,27

- Thème:(01) – Contrats – 2,27

1. Il doit y avoir une possibilité de maintenance curative des LAN (équipements et liaisons) en interne ou en externe à l'organisation.

2. On doit prévoir des contrats de maintenance pour tous les matériels informatiques et au moins pour ceux sensibles.

3. Les dépannages doivent être effectivement rapides (moins de 24 heures réparation comprise).

4. Des contrats de maintenance sont requis pour tous les logiciels de base installés (système d'exploitation, système réseau, ponts, passerelles et interfaces, gestion des données, etc.).

5. Un centre technique de support maintenance interne ou externe doit être créé (et d'aide, d'une manière générale), fournissant une assistance téléphonique rapide et il doit exister des procédures d'accès restrictif et de contrôle spécifique en cas de télé-maintenance.

6. Un carnet de maintenance doit être maintenu (matériel et logiciel), propriété de l'organisation, tenu à jour de toutes les interventions de la maintenance des constructeurs et opérateurs (modifications effectuées, nom et signature du technicien).

Facteur 601: Les protocoles de graduation – 2,16

- Thème:(01) - Procédure de graduation – 2,80

1. On doit procéder à des tests de validation sur une machine dédiée pour les logiciels (achetés ou d'origine interne), la réception finale étant confiée au détenteur ou responsable utilisateur adéquat.

2. On doit procéder systématiquement à une copie de sauvegarde du logiciel ainsi testé (quelquefois fournie par l'éditeur).

- Thème:(02) – Graduation des applications – 2,00

3. En cas de développement d'application il doit y avoir séparation de l'environnement développement, de l'environnement test et de l'environnement exploitation.

4. En cas de développement d'application par l'utilisateur lui-même, celui-ci devrait effectuer des essais avant l'exploitation des programmes.

5. En cas de développement d'application par un fournisseur ou par un autre utilisateur on doit définir un protocole de recette (jeu d'essais, documentation, régime de sauvegarde, etc.) entre le développeur et utilisateur. Ce protocole devra être conforme au protocole interne en matière d'intégration de la sécurité dans le développement. On vérifiera donc en particulier le respect formel des consignes de sécurité (Cf. facteur 602).

6. On doit vérifier que le niveau de sécurité offert (au moins décrit, si possible testé) correspond bien aux spécifications fonctionnelles en se basant sur un protocole formalisé d'évaluation de la sécurité du système reposant sur les méthodes d'assurance qualité et conformité (exemple : ITSEC).

Facteur 602: Les méthodes d'analyse-programmation – 1,89

- Thème:(01) – Méthodes d'analyse-programmation – 1,89

1. Chaque projet doit faire l'objet d'un avant-projet et d'un cahier des charges élaborés avec le concours des utilisateurs en liaison avec le représentant des tiers.

NB : Il convient d'assurer la conception et la réalisation dans le cadre de la méthode d'assurance qualité de l'organisation, en respectant les normes d'exploitation et d'installation sécurisées.

2. La conception (et la réalisation) de l'application doit intégrer les spécifications de sécurité qui résultent elles-mêmes d'une analyse méthodique et formelle des menaces potentielles.

3. On doit prévoir une documentation (application) structurée, claire et tenue à jour (aussi bien pour l'utilisateur que pour ceux de la maintenance).

4. Des règles précises sont requises pour développer une application (langage, progiciels standard, tableurs, etc.).

5. En cas de développement par un fournisseur, le choix de celui-ci doit être basé sur la capacité d'évolution.

6. Les sources des développements doivent demeurer la propriété de l'organisation, quel que soit le développeur.

Facteur 603: Les contrôles programmés – 1,50

- Thème:(01) - Choix et cohérence des contrôles – 1,33

1. On doit faire au moment de l'étude fonctionnelle de chaque application, une étude quantitative des conséquences d'erreur ou d'action malveillante sur chaque type de données stratégiques.

NB : Cette étude sert de fondement au choix de la nature des contrôles qui devront être inclus dans le logiciel.

2. On doit vérifier la cohérence des contrôles sur chaque type de donnée stratégique dans tous les programmes où cette donnée peut être mise à jour.

3. Les contrôles ci-dessus doivent générer des "alertes", effectivement prises en compte par les utilisateurs, et vérifiées par les responsables dans un délai ne remettant pas en cause l'efficacité des alertes déclenchées.

- Thème:(02) - Contrôles programmés – 1,75

4. Pour les données stratégiques, il doit y avoir des contrôles de base (cadrage, limites de valeur, vraisemblance simple.

5. Pour les données stratégiques, il doit y avoir des contrôles de vraisemblance directe (fourchettes).

6. Il doit y avoir pour les données stratégiques, des contrôles de vraisemblance indirecte (ratios).

7. Pour les données stratégiques, il doit y avoir des contrôles de cohérence (évolution et comparaison par rapport à des données antérieurs ou à une base statistique).

Facteur 604: La sécurité des progiciels – 2,00

- Thème:(01) - Les progiciels – 2,00

1 Le choix des progiciels doit reposer sur des études comparatives (sites déjà équipés, enquêtes, etc.) de fiabilité, de qualité et de sécurité.

2 Le choix des progiciels doit reposer sur la capacité des fournisseurs à maintenir et à faire évoluer les produits.

3 On doit tester, sur des bases réelles ou quasi réelles, le progiciel avant son acquisition sur une période suffisamment longue pour permettre une appréciation fondée (notamment sur les fonctions de sécurité).

4 Un contrat doit permettre une possibilité de récupération des programmes sources documentés en cas de défaillance du fournisseur.

5 On doit faire en sorte que les modifications des progiciels, spécifiques pour votre organisation ("spécificités maison"), ne soient pas un obstacle à la mise en oeuvre des versions suivantes.

6 Les contrats doivent prévoir la fourniture d'une documentation ad hoc (fonctionnelle, d'exploitation et utilisateurs), ainsi qu'un minimum de formation au démarrage.

7 On doit vérifier que la documentation décrit clairement et formellement les services et mécanismes de sécurité (ainsi que le mode d'exploitation sécuritaire) incorporés dans le progiciel.

8 On doit vérifier la conformité de l'offre sécurité avec les spécifications requises.

9 Les progiciels stratégiques doivent être certifiés et scellés (éventuellement chiffrés).

Richard Pagé

Coordonnateur ministériel de la sécurité de l'information

Direction générale des services à la gestion

700 boul. René-Lévesque Est (14e étage)

Québec (Québec) G1R 5H1

(418) 646-3043

rpage@mtq.gouv.qc.ca