

Catégorisation des documents et autres actifs informationnels aux fins de la protection des renseignements personnels et de la sécurité

Guide Trousse d'outils

Avertissement

Vous êtes invités à soumettre vos commentaires auprès du coordonnateur régional de la sécurité des actifs informationnels de votre Agence.

Si vous l'utiliser comme référence, vous êtes priés d'ajouter, après le numéro et le titre du guide, la mention « guide approuvé, version [1.3] du [2006-09-22] ».

STATUT : Approuvé (Version 1.3 – 2006-09-22)

APPROBATION : Le 2006-03-23 par la table des coordonnateurs régionaux des actifs informationnels (TCRSAI)

Remplace le standard : MSSS04-021 version 1.3 – 2006-03-29

L'original sera signé par : Philippe Moss _____

Date de mise en vigueur : 2006-09-25

Date de révision : 2009-04-25

MSSS04-021 Guide de Catégorisation des documents et autres actifs informationnels

*Direction des ressources informatiques
Direction générale de la coordination, du financement, de l'équipement
et des ressources informationnelles*

Guide de la catégorisation des documents et autres actifs informationnels aux fins de la protection des renseignements personnels et de la sécurité

Guide de sécurité de l'information

Responsable de la production du présent guide :

Philippe Moss
Directeur adjoint

Éditeur : Pierre P. Tremblay, ing. PSI RSSS

Auteur :

Ce guide a été élaboré par l'équipe de droit du cyberspace du Centre de recherche en droit public de l'Université de Montréal à partir du modèle proposé dans le Guide relatif à la catégorisation des documents technologiques en matière de sécurité du Secrétariat du Conseil du Trésor.

Ce guide a été révisé et adapté par Jacques Bergeron, chargé de projet pour SOGIQUE en mars 2004, en juin 2005 et en novembre 2005.

M. Jacques Bergeron

Titre :

Société : Groupe Conseil GSR

TCRSAI

Sous-comité TCRSAI révision

Approuvé 20 septembre 2005

Novembre 2005

Membres du comité de lecture et de validation de la version 1,3 février 2006 :

Jocelyne Legras

ASSS Capitale Nationale

Nathalie Malo

ASSS Lanaudière

Alain Boisvert

ASSS Estrie

Jacques Bergeron

Groupe Conseil GSR

Jean Laterrière

Sogique

Pierre P. Tremblay

MSSS

Dans ce document, le générique masculin est utilisé pour simplifier la lecture du texte, mais s'applique autant pour le féminin que pour le masculin.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

Pour toute question ou commentaire, veuillez communiquer avec votre coordonnateur régional de la sécurité de l'information.

Remerciements

L'équipe de réalisation tient à remercier toutes les personnes ayant collaboré avec elle.

Éditeur : Direction des ressources informatiques
Ministère de la Santé et des Services sociaux
1075 chemin Ste-Foy – 4^e étage
Québec (Québec) G1S 2M1

© Direction des ressources informatiques, ministère de la Santé et des Services sociaux, Québec, 2006

Toute reproduction totale ou partielle de ce document est autorisée à condition d'en mentionner la source

Numéro de classification :

Date de publication: OCTOBRE 2006
Date de mise en vigueur : 2006-09-25

Historique du document :

Version	Date	Modification	Par
1,1	2004-02-12	Révision pour inclure la PRP	Jacques Bergeron
1,2	2005-06-15	Mise à jour suite aux commentaires de la TCRSAI	Jacques Bergeron
1,3	2005-10-24	Mise à jour suite aux commentaires du sous-comité	Jacques Bergeron
	2006-03-17	Exemple tableau disponibilité page 55	Pierre P. Tremblay
	2006-09-22	Ajout calcul % disponibilité page 55 et 56	Pierre P. Tremblay

Catégorisation du document :

Disponibilité : niveau 1 – bas

Intégrité : niveau 2 - moyen

Confidentialité : niveau 1 - bas

Diffusion du document :

Diffusion : Internet

Adresse Internet : www.msss.gouv.qc.ca

Conservation : 5 ans après le remplacement par une nouvelle version

Nom du fichier source du document : MSSS04-021 Guide de catégorisation v1,3 vapprouvée 2006-10-05.doc

Demande de modification

Numéro : 003

Date : 2005-10-08

Demandée par : PSI RSSS

Organisme : MSSS

Description de la demande :

Ajuster le guide de la catégorisation des documents et autres actifs informationnels aux fins de la protection des renseignements personnels et de la sécurité en fonction des changements apportés au processus de catégorisation qui fut simplifié en regroupant les documents par processus d'affaires.

Raison :

Les documents impliqués dans un même processus d'affaires doivent généralement avoir les mêmes valeurs de catégorisation en terme de disponibilité. En regroupant les documents par processus d'affaires l'opération de catégorisation est grandement simplifiée puisque le nombre de processus d'affaires est d'un ordre de magnitude de moins que le nombre de document.

Suggestion :

Liste des changements entre la version 2006-02-28 et 2006-03-17 :

Anick Monette/RR/Reg13/SSSS : les exemples dans le tableau Disponibilité de l'annexe 1 à la page 55 pour le niveau 3 sont erronés. Par exemple que « les documents soumis à un délai de conservation » n'est pas un critère par la catégorisation à un niveau 3 de disponibilité (D). Par exemple, une facture payée d'il y a 2 ans a une catégorisation de D=1 donc peut être envoyée à un entrepôt à l'extérieur.

Liste des changement entre la version 2006-03-29 et 2006-09-22 :

Daniel.Pelletier@msss.gouv.qc.ca : Formules pour le calculs des % de disponibilité à ajouter au MSSS04-21

Table des matières

1. CONTEXTE	1
2. OBJECTIF DU GUIDE	3
2.1 OBJECTIF	3
2.2 AUDIENCE	4
2.3 LIMITATIONS	4
2.4 SOUTIEN	5
2.5 POSITIONNEMENT DU PROCESSUS DE CATÉGORISATION	5
3. PROCESSUS DE MISE EN OEUVRE	13
3.1 LES ACTEURS	13
3.2 ÉQUIPES DE MISE EN OEUVRE.....	14
3.2.1 <i>Équipe de projet</i>	15
3.2.2 <i>Équipes de détenteurs</i>	16
3.2.3 <i>Équipe de collaborateurs</i>	17
3.2.4 <i>Équipe de validation</i>	18
3.2.5 <i>Comité de PRP et de sécurité</i>	18
4. PROCESSUS DE CATÉGORISATION.....	19
4.1 PLANIFICATION DU PROJET ET ORGANISATION DU PROJET	20
4.1.1 <i>Réunion du comité de PRP et de sécurité et définition du projet</i>	20
4.1.2 <i>Présentation du projet à la direction générale</i>	20
4.1.3 <i>Préparation du projet</i>	21
4.1.4 <i>Coordination de l'équipe de projet</i>	21
4.1.5 <i>Réunion de démarrage</i>	21
4.2 PRÉPARATION DE L'EXERCICE DE CATÉGORISATION	23
4.2.1 <i>Recensement des informations et identification des unités administratives</i>	23
4.2.2 <i>Valider l'étendue de la catégorisation</i>	25
4.2.3 <i>Prise de contact avec les détenteurs</i>	25
4.2.4 <i>Le recensement des lois sectorielles</i>	28
4.2.5 <i>La vérification à l'assujettissement du secteur à des ententes contractuelles</i>	30
4.2.6 <i>La vérification des directives propres au secteur</i>	31
4.3 PRISE DE L'INVENTAIRE DES DOCUMENTS.....	32
4.3.1 <i>Les fondements</i>	32
4.3.2 <i>Les techniques de documentation des processus d'affaires</i>	37
4.3.3 <i>Exemple d'application</i>	39
4.4 CATÉGORISATION DES DOCUMENTS OU GROUPES DE DOCUMENTS	46
4.4.1 <i>Préparation à l'exercice</i>	46
4.4.2 <i>Le processus de catégorisation</i>	48
4.4.3 <i>Définition et explications des seuils d'impact</i>	48
4.4.4 <i>Évaluer les seuils d'impact</i>	51
4.4.5 <i>Formulaire utilisé</i>	52
4.4.6 <i>Exemple d'application</i>	54
4.5 CONSIGNATION DES RÉSULTATS	57
4.5.1 <i>Critères de sélection</i>	57
4.5.2 <i>Exemple d'application</i>	60
4.6 ANALYSE ET VALIDATION DES RÉSULTATS.....	62
4.7 PRÉSENTATION ET APPROBATION DES RÉSULTATS.....	63
5. CONCLUSION.....	64
ANNEXE 1 DÉFINITION DES SEUILS D'IMPACT	66

ANNEXE 2 LEXIQUE	75
ANNEXE 3 LISTE DES PRINCIPALES LOIS RÉGISSANT LE RÉSEAU SOCIO SANITAIRE QUÉBÉCOIS OU AYANT UN IMPACT SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS	85
ANNEXE 4 EXEMPLAIRE DU	87
« FORMULAIRE D'INVENTAIRE ET DE CATÉGORISATION »	87
ANNEXE 5 EXEMPLAIRE DE LA	89
« MATRICE DE CATÉGORISATION »	89

1. Contexte

Les établissements et organismes du domaine de la santé et des services sociaux sont tenus à plusieurs obligations concernant les documents et autres actifs informationnels qu'ils ont en leur possession, qu'ils contrôlent ou qu'ils alimentent, notamment d'assurer la protection des renseignements personnels et leur sécurité. Ils ont donc à prendre les mesures requises afin d'assurer à ces documents une protection adéquate compte tenu de ces obligations. De plus, tant en raison des exigences relatives aux informations sensibles qu'en raison des impératifs de bonne gestion et des règles d'éthique régissant les professionnels de la santé, la protection des renseignements personnels et la sécurité des documents et autres actifs informationnels¹ demeure une préoccupation majeure des intervenants oeuvrant dans le domaine de la santé. Étant donné l'importance stratégique des systèmes d'information utilisés par les établissements et les organismes², de même que la nature sensible des renseignements qu'ils traitent, la sécurisation des documents et autres actifs informationnels devient un enjeu stratégique pour le réseau sociosanitaire.

Dans cette perspective, le ministère de la Santé et des Services sociaux a récemment adopté le **« Cadre global de gestion des actifs informationnels appartenant aux établissements du réseau de la santé et des services sociaux – Volet sur la sécurité »** (appelé ci-après « Cadre global-Volet sécurité »). Le Cadre global-Volet sécurité vise à communiquer les attentes, les obligations et les rôles de chacun des intervenants en matière de sécurité des documents et autres actifs informationnels. À ce titre, les établissements ont notamment l'obligation de se doter d'une politique de sécurité. Le ministère a aussi élaboré un document portant sur la protection des renseignements personnels. Ce document s'intitule **Cadre global de gestion des actifs informationnels appartenant aux établissements du réseau de la santé et des services sociaux – Volet sur la protection des renseignements personnels »** et dénote l'inclusion de la dimension « protection des renseignements personnels » dans l'approche de sécurité. Ce second volet inclut la **« Politique nationale de protection des renseignements personnels des établissements du réseau de la santé et des services sociaux »**.

¹ Les notions de « document », de « document technologique » et d'« actif informationnel » sont définies au lexique.

² Dans un souci d'allègement du texte, nous utiliserons uniquement le terme « établissements » pour désigner l'ensemble des organisations du secteur sociosanitaire assujetti à l'application du Cadre global, art. 2.

Afin de les appuyer dans leurs efforts, le ministère a créé en octobre 2001 la « Table des coordonnateurs régionaux en sécurité » afin d'échanger et de partager quant aux enjeux reliés au déploiement du Cadre global en général. Or, la responsabilité de sécuriser les actifs informationnels revient aux détenteurs respectifs de ces actifs. Afin de supporter les établissements, la Société de gestion informatique SOGIQUE inc. a été mandatée pour développer une trousse destinée à accompagner et à supporter les établissements dans l'implantation du Cadre global.

En août 2002, le ministère autorisait une étude afin de mettre au point une politique sur la protection des renseignements personnels. Les établissements publics sont, en effet, en ce qui concerne les renseignements et documents qui sont en leur possession, liés par des devoirs et obligations énoncés dans les lois, davantage que les entreprises privées. Dès lors, pour les établissements, les impératifs de protection des renseignements personnels et de sécurité ne sont pas uniquement des risques à gérer mais sont également des obligations formelles pour lesquelles il leur incombe de prendre les moyens conséquents.

C'est dans ce contexte que le présent guide de « Catégorisation des documents et autres actifs informationnels aux fins de la protection des renseignements personnels et de la sécurité » a été développé. Le terme Catégorisation utilisé dans ce document est employé au sens de Classification dans le Cadre global.

Le guide s'inspire, pour des fins de cohérence et d'uniformité, de la structure du Guide relatif à la catégorisation des documents technologiques en matière de sécurité, version 1.2 du 26 octobre 2003, élaboré sous l'égide du Secrétariat du Conseil du trésor (SCT), auquel les établissements ne sont pas par ailleurs formellement subordonnés.

2. Objectif du guide

2.1 Objectif

L'objectif du présent guide est de fournir aux établissements une méthodologie et des outils leur permettant d'inventorier les actifs informationnels, selon la gravité des impacts résultant d'un bris de sécurité ou de protection des renseignements personnels (PRP) pour l'une ou l'autre des trois obligations faites aux établissements : **1) la disponibilité de l'information, 2) l'intégrité de l'information et 3) la confidentialité de l'information**³.

Les établissements du réseau de la santé et des services sociaux détiennent des actifs informationnels, documents ou autres dossiers. La nature des informations contenues par ceux-ci assujettit les établissements à des obligations juridiques et professionnelles, que ce soit de par la nature personnelle ou confidentielle de certaines informations ou par des obligations découlant de textes spécifiques. Les actions ou les inactions des établissements sont encadrées par le droit.

De plus, la nature de certaines informations manipulées peut, en cas de problèmes liés à ces informations, mettre en péril la capacité de l'établissement à remplir adéquatement sa mission. Ce dernier peut également être exposé à des conséquences économiques ou sociales.

La catégorisation de l'information permet de :

- Définir clairement les types d'actifs informationnels pour lesquels un niveau de protection particulier est requis ;
- Identifier les actifs informationnels qui seront sélectionnés afin d'effectuer l'analyse de risques (cette activité est couverte dans le troisième guide intitulé « Guide d'élaboration d'un plan directeur de sécurité de l'information - Trousse d'outils ») et préciser quelles dimensions seront retenues pour les fins d'analyse (dimensions de disponibilité, d'intégrité et de confidentialité) ;

³ Ces trois éléments sont représentés par l'acronyme « DIC » tout au long de ce texte.

- Faciliter l'identification et l'évaluation périodique des risques afin de s'assurer de l'adéquation des mécanismes de PRP et de sécurité en vigueur avec les risques encourus, en fournissant les outils permettant de réaliser la catégorisation préalable à ces évaluations de risques.

2.2 Audience

Ce guide s'adresse principalement aux personnes suivantes :

- Le responsable à qui la tâche de mener l'exercice de catégorisation des actifs informationnels a été assignée ;
- Le dirigeant de l'établissement ou son représentant ;
- Le responsable de la sécurité des actifs informationnels (RSAI) ;
- Le directeur de la gestion des ressources informationnelles ;
- Les détenteurs de documents et autres actifs informationnels ;
- Le responsable des archives ;
- Le professionnel en sécurité de l'information ;
- Le responsable de l'accès et de la protection des renseignements personnels.

2.3 Limitations

La disparité entre les établissements et les différents stades d'avancement des activités de gestion, reliées à la protection des renseignements personnels et à la sécurité de l'information, au sein de chacun des établissements, fait en sorte que le guide devra être adapté et ne devra en aucun cas se substituer au jugement professionnel des intervenants. Il faut toutefois rappeler que les lois imposent aux établissements des devoirs à l'égard des actifs informationnels qui sont en leur possession. Les mesures de protection des renseignements personnels et de sécurité appropriées aux enjeux doivent donc impérativement être mises en place pour s'assurer du respect des obligations juridiques et médicales des établissements.

2.4 Soutien

Les Agences de développement de réseaux locaux de services de santé et de services sociaux ont le mandat de supporter les établissements dans leur démarche d'élaboration de politiques de PRP et de sécurité de l'information.

2.5 Positionnement du processus de catégorisation

Lorsqu'un établissement procède à une démarche d'analyse de risques, il désire s'attarder aux actifs informationnels qui supportent sa mission et ses activités les plus importantes. Il voudra ainsi catégoriser les actifs informationnels qui ont une plus grande valeur pour lui.

Un des objectifs visés par la démarche de catégorisation est d'attribuer un niveau d'impact pour chacun des critères du DIC. Ce niveau d'impact est une évaluation de la valeur de l'actif informationnel pour l'établissement. En effet, plus la perspective de l'impact d'un événement est importante, plus la valeur d'un actif informationnel est élevée. Bien que la catégorisation soit une étape importante de la protection et de la sécurisation des actifs informationnels, cette dernière à elle seule ne suffit pas. La catégorisation est une phase s'inscrivant dans une démarche intégrée de PRP et de sécurité des actifs informationnels. La **figure 1** illustre cette démarche.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

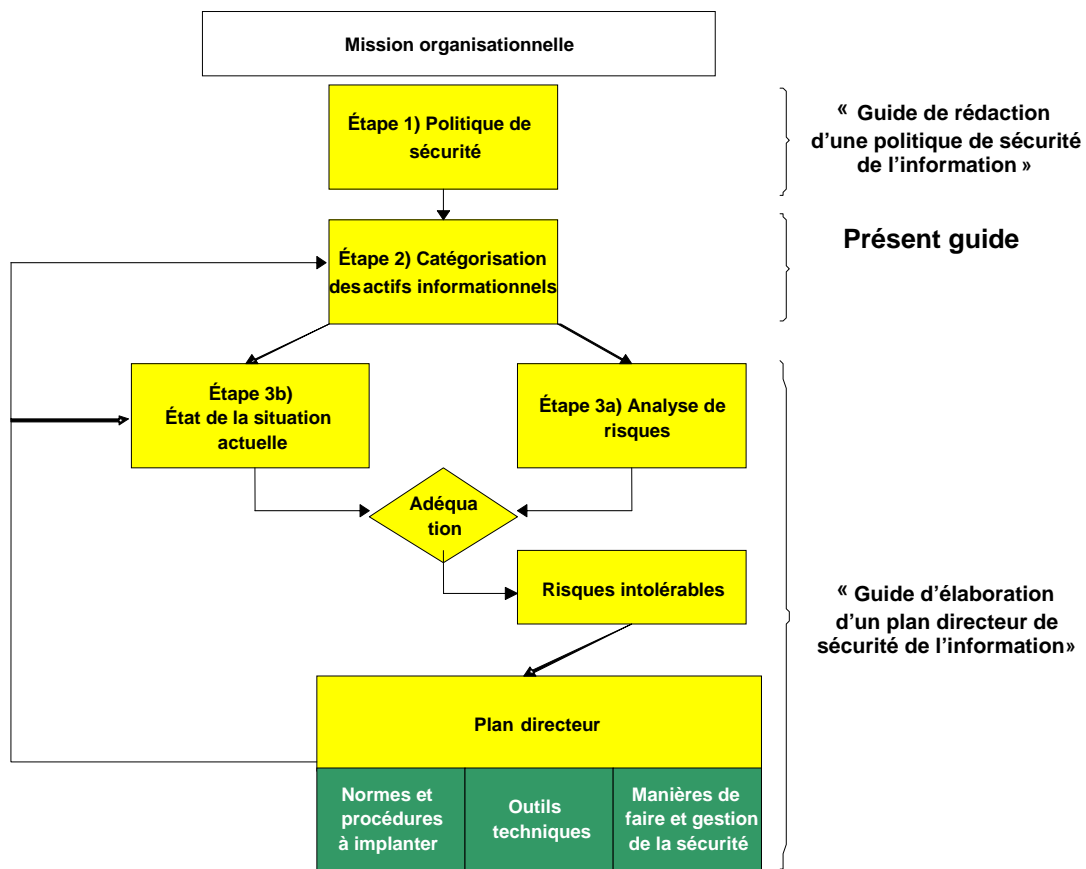


Figure 1 – Positionnement du processus de catégorisation

L'élaboration de la politique **de sécurité**, qui énonce les grandes orientations et obligations d'un établissement en matière de sécurité, précède toute activité.

La catégorisation, quant à elle, est l'étape qui précède l'étape 3a) - analyse de risques. Elle permet de préciser quels sont les actifs informationnels qui sont importants pour l'établissement et pour lesquels une analyse de risques est nécessaire. En effet, un établissement ne peut protéger tous les actifs informationnels manipulés par les personnes ou traités par les systèmes d'information. Il doit être en mesure d'identifier les actifs les plus importants et mettre en place des mesures appropriées pour les protéger contre la matérialisation des risques les plus pertinents.

À cette fin, l'analyse de risques permet de déterminer quels sont les risques les plus probables qui peuvent se matérialiser et affecter un établissement. Quand à elle, l'évaluation de la situation actuelle (étape 3b) permet de déterminer si les mesures de PRP et de sécurité mises en place permettent d'adresser adéquatement les risques identifiés. Enfin, le plan directeur (étape 3c) vise à élaborer des actions correctrices si les mesures sont inadéquates et à en établir la priorité.

La démarche de catégorisation sert ainsi à établir la valeur de tous les actifs informationnels détenus par un établissement et à recenser ceux pour lesquels une analyse de risques sera effectuée. De plus, la démarche de catégorisation permet de cibler les scénarios de risques en fonction des dimensions retenues pour chacun des actifs informationnels. Ces dimensions sont :

1. La disponibilité de l'information ;
2. L'intégrité de l'information ;
3. La confidentialité de l'information.

Ces trois dimensions sont définies dans une section ultérieure.

Les résultats de la démarche de catégorisation servent d'intrants à l'analyse de risques et à l'état de la situation actuelle. La **figure 2** illustre ces concepts.

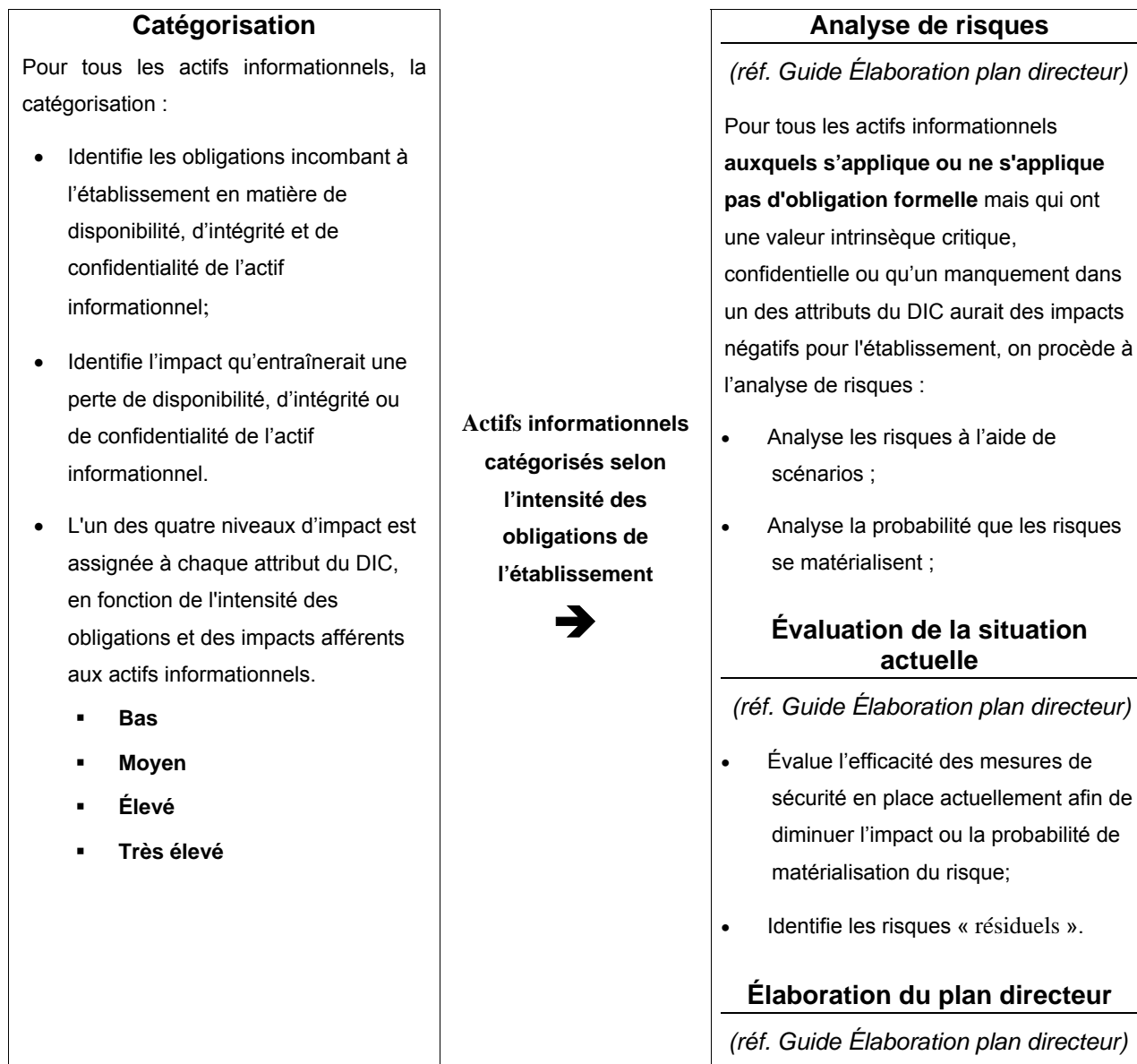


Figure 2 – Relations entre la catégorisation, l'analyse des risques et l'état de la situation actuelle

2.6 Les définitions des concepts utilisés

2.6.1 La disponibilité, l'intégrité et la confidentialité de l'information

Ces concepts sont centraux dans la démarche de catégorisation. Les responsables du projet doivent ainsi s'assurer de les maîtriser adéquatement.

La disponibilité de l'information

Selon la définition du Cadre global, la disponibilité de l'information est la **propriété qu'ont les données, l'information et les systèmes d'information et de communication, d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.**

En fait, la disponibilité de l'information réfère à la propriété de l'information d'être **accessible** selon les besoins d'affaires de l'établissement.

L'intégrité de l'information

Selon la définition du Cadre global, l'intégrité de l'information est la **propriété d'une information ou d'une technologie de n'être ni modifiées, ni altérées, ni détruites d'une façon erronée ou non autorisée.**

Nous retrouvons ici plusieurs concepts importants.

- En premier lieu, l'information doit être **exacte**. Elle doit donc être **conforme** à ce qu'elle doit représenter.
- En second lieu, l'information doit être **complète, c'est-à-dire intégrale et exhaustive**. Ainsi,
 - **Tous les documents doivent être présents ;**
 - **L'ensemble des champs d'information nécessaires sont complétés à l'intérieur de chaque document.**

Les contrôles d'application permettent habituellement d'atteindre ces objectifs. Les contrôles d'accès spécifiques aux applications sont également importants à considérer.

- L'information inscrite/enregistrée doit être autorisée. À cette fin, l'information ne doit pas être fausse, non authentique ou avoir été modifiée de façon intentionnelle.

Encore ici, les contrôles d'accès spécifiques sont à considérer pour atteindre cet objectif.

Cette dimension est applicable autant pour les documents sur support papier que les documents électroniques enregistrés dans les bases de données de l'établissement.

La confidentialité de l'information

Selon la définition provenant du Cadre global, la confidentialité **est la propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservées à des personnes ou entités désignées et autorisées.**

La **divulgation** de l'information doit être effectuée à des personnes autorisées selon les règles établies par l'organisme. De plus, les obligations de PRP sont incluses dans la dimension de confidentialité.

2.6.2 Actif informationnel

Un actif informationnel est composé de deux éléments :

1. Le document ;
2. La composante sur laquelle se trouve le document.

Un document peut être sur support papier. Par exemple, la prescription remplie par le médecin est un document sur support papier. Le document peut également être sur support électronique. Par exemple, la prescription qui est saisie dans un système et qui est entreposée dans une base de données devient un document électronique. Enfin, les rapports imprimés provenant d'un système d'information sont des documents sur support papier.

Les composantes sont les endroits physiques ou logiques où sont contenus les documents. Ainsi, le dossier physique est une composante. Ce dossier physique peut être entreposé dans un classeur qui devient également une composante. Le classeur se trouve dans un local. Ce dernier devient donc aussi une composante. Dans le même ordre d'idées, le document électronique est entreposé dans une base de données qui devient une composante. Un logiciel d'application traite le document électronique et devient une composante. La base de données est située sur un serveur et ce dernier est localisé dans une salle informatique. Le serveur et la salle informatique deviennent des composantes. Il est important de recenser toutes les composantes qui supportent un document papier ou électronique car la démarche d'évaluation de la situation actuelle exige d'évaluer les contrôles en place sur chacune des composantes supportant des documents qui ont été catégorisés comme étant importants pour l'établissement.

Les composantes peuvent également être de nature commune. On les désigne comme étant des actifs communs. Par exemple, si dans l'établissement les courriels qui sont échangés sont considérés comme étant importants sur le plan de la disponibilité, de l'intégrité et/ou de la confidentialité, le système de courrier électronique devient une composante importante, le serveur où se trouve ce système est une composante importante et la salle physique où se trouve le serveur devient une composante importante.

Ainsi, on peut retrouver les actifs communs suivants :

- 1 Le site Internet (et les composantes rattachées comme le système, la base de données, le serveur et la salle informatique);
- 2 Le réseau local de télécommunication et les composantes comme le câblage, les équipements de télécommunication, la salle physique où se trouvent les équipements;) ,
- 3 Les systèmes de téléphonie et de communication interne.

La démarche exige également la prise d'inventaire et la catégorisation des documents qui peuvent être entreposés sur des portables ou des ordinateurs de table.

Cependant, il faut faire attention de ne pas inventorier et catégoriser des éléments qui sont des mesures de protection plutôt que des actifs informationnels. Par exemple, les gardes-barrières, les anti-virus ne supportent pas les processus d'affaires. Ces éléments ne contiennent pas d'informations nécessaires aux processus d'affaires. Ce sont plutôt des mesures de contrôle et de protection contre des menaces potentielles qui pourraient affecter la disponibilité, l'intégrité ou la confidentialité des informations manipulées par les processus d'affaires et mettre ainsi en péril la mission ou l'image de l'établissement.

L'efficacité de ces mesures de contrôle sera évaluée lors de l'étape d'évaluation de la situation actuelle.

3. Processus de mise en oeuvre

3.1 Les acteurs

La catégorisation de l'information est un processus important qui exige, pour être mené à bien, l'engagement de la direction générale ainsi que la collaboration et le soutien de plusieurs intervenants de l'établissement, tels que :

- Les gestionnaires des unités administratives utilisatrices des actifs informationnels ;
- Les responsables de PRP et de sécurité ;
- Les utilisateurs principaux (ou pilotes) ;
- Le dirigeant de l'établissement ou son représentant.

Conseil d'administration et direction générale

En tant que premier acteur, le conseil d'administration de l'établissement doit exprimer clairement, par le biais de la direction générale, sa volonté de mener à terme le projet de catégorisation des documents en matière de PRP et de sécurité et d'implanter un processus continu de catégorisation, par exemple si un nouveau système d'information est implanté. Le directeur général doit préciser par écrit (ou autrement) la décision de réaliser le projet de catégorisation à tous les niveaux de l'établissement.

Comité de PRP et de sécurité de l'établissement

L'implication de ce comité est primordiale. Ce dernier est responsable du projet de catégorisation auprès de la direction générale de l'établissement. Il informe celle-ci du déroulement du projet. Pour ce faire, des réunions périodiques doivent avoir lieu avec le chargé de projet.

Chargé de projet

Le chargé de projet est une personne nommée par la direction générale de l'établissement afin de prendre en charge la démarche de catégorisation, c'est-à-dire planifier, organiser, diriger et contrôler les activités de catégorisation.

Participation des détenteurs et des unités administratives

La participation des détenteurs et des unités administratives utilisatrices des actifs informationnels est essentielle afin qu'ils puissent statuer sur la valeur de l'information qu'ils gèrent. Le processus de catégorisation donnera des résultats en fonction des besoins exprimés et approuvés.

3.2 Équipes de mise en oeuvre

La figure 3 illustre la structure organisationnelle proposée pour la réalisation du projet de catégorisation. Cette structure pourra être adaptée en fonction du contexte de l'établissement.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

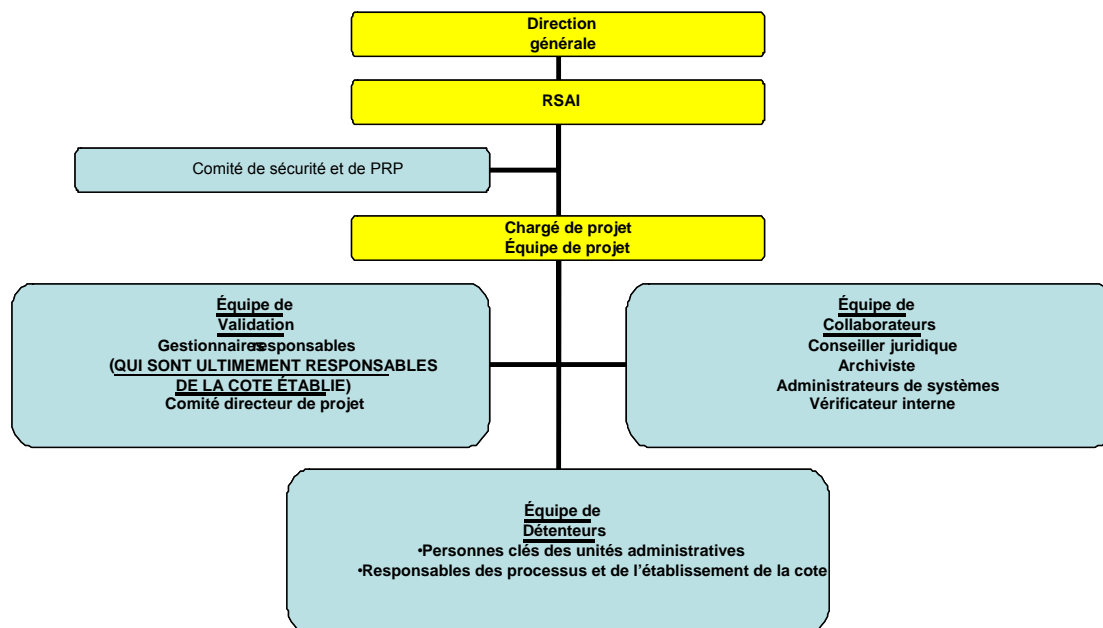


Figure 3 – Structure organisationnelle du projet

On peut ainsi envisager de mettre sur pied quatre types d'équipes de travail pour la réalisation de la catégorisation, soit une équipe de projet de base, des équipes de détenteurs, une équipe de collaborateurs et une équipe de validation.

3.2.1 Équipe de projet

L'équipe de projet, chargée de la réalisation de la catégorisation, est composée du chargé de projet, du responsable de la PRP, du responsable de la sécurité des actifs informationnels (RSAI), du dirigeant de l'établissement ou son représentant et du responsable des archives. Cette équipe supporte le chargé de projet.

Les responsabilités de cette équipe comprennent entre autres :

- La planification des activités et l'échéancier de travail ;
- La cueillette des renseignements requis ;

- L'organisation et l'animation des entrevues et des ateliers de travail ;
- La production des documents de travail ;
- La consolidation et la présentation des résultats.

3.2.2 Équipes de détenteurs

Les équipes de détenteurs sont composées des personnes clés des unités administratives visées par la catégorisation. Les détenteurs sont en mesure d'évaluer les impacts réels d'incidents potentiels pouvant affecter la DIC des actifs utilisés dans leur propre unité administrative. Ces dernières sont reliées de près ou de loin à la mission de l'établissement et suivent l'organigramme de l'établissement. Par exemple, on pourrait retrouver les unités suivantes : laboratoire, psychiatrie, approvisionnement, diététique, services administratifs, etc. Habituellement, les détenteurs sont identifiés pour l'ensemble de ses missions. On peut retrouver, selon le type d'établissement, les missions suivantes :

1. La mission clinique de l'établissement ;
2. La mission recherche de l'établissement ;
3. La mission évaluation technologique (biomédical) de l'établissement ;
4. La mission enseignement de l'établissement ;
5. La mission service public de l'établissement.

Sans la participation des détenteurs, il sera difficile pour l'équipe de projet de réaliser l'exercice de catégorisation. Ils connaissent habituellement très bien les actifs informationnels et ont élaboré des procédures de gestion en fonction de l'importance de ces actifs informationnels.

Les tâches des détenteurs sont de fournir les renseignements pertinents concernant les actifs informationnels ainsi que sur l'environnement spécifique de leur unité d'affaires, participer aux

ateliers de travail pour remplir la matrice de catégorisation, commenter les documents de travail et proposer au besoin des solutions.

Le responsable des services informatiques doit être considéré comme un détenteur. Il est détenteur des actifs informationnels suivants :

1. Les équipements informatiques centralisés ;
2. Les équipements de télécommunication ;
3. Les logiciels de base et les utilitaires ;
4. Les logiciels communs (courriels) ;
5. Les outils de développement et de gestion des environnements ;
6. Les systèmes de gestion de bases de données ;
7. Les logiciels de support (copies de sécurité) ;
8. Les imprimantes (si l'impression est centralisée) ;
9. La documentation des systèmes (applicatifs et de base).

3.2.3 Équipe de collaborateurs

L'équipe de projet est appuyée par une équipe de collaborateurs qui est consultée selon le cas ou de manière ponctuelle. L'équipe de collaborateurs inclura au besoin un conseiller juridique, un spécialiste en gestion documentaire, un vérificateur, un administrateur de systèmes ou toute autre personne dont l'expertise sera jugée pertinente.

Entre autres, les tâches suivantes sont réalisées par cette équipe :

- L'apport de renseignements relatifs à des exigences légales ou à des contraintes spécifiques de l'environnement de l'établissement (lois sectorielles, exigences découlant de la Lssss, *Loi sur l'accès*, délais de conservation, systèmes d'information, etc.) ;
- L'apport de son expertise à l'équipe de projet de base pour des questions spécifiques ;
- L'apport de documents de travail et suggérer des solutions, au besoin.

Il est également important que les détenteurs et les gestionnaires des unités administratives visées par la catégorisation (ou leur représentant désigné) participent à un atelier de travail afin de valider l'évaluation des documents de leur unité.

3.2.4 Équipe de validation

L'équipe de validation est composée de gestionnaires désignés responsables des unités administratives visées par la catégorisation.

Des représentants de la DSP (Direction des soins professionnels) et de la DSI (Direction des soins infirmiers) doivent également faire partie de l'équipe de validation.

Les tâches de cette équipe de validation sont de revoir et de valider les travaux de catégorisation effectués.

3.2.5 Comité de PRP et de sécurité

Ce comité est responsable de valider les documents finaux produits par l'équipe de projet et de recommander la présentation des résultats au comité de direction de l'établissement.

4. PROCESSUS DE CATÉGORISATION

L'activité de catégorisation est une étape préalable qui permettra d'attribuer à chaque « document papier ou électronique » une cote d'impact reflétant les obligations qui y sont associées et son importance pour le bon fonctionnement de l'établissement. Tel que mentionné auparavant, les résultats de la catégorisation seront utilisés comme intrants à la phase de l'analyse des risques prévue dans le « Guide d'élaboration du plan directeur de sécurité de l'information - Guide Trousse d'outils ». Le processus de catégorisation comprend sept étapes qui sont présentées à la figure 4.

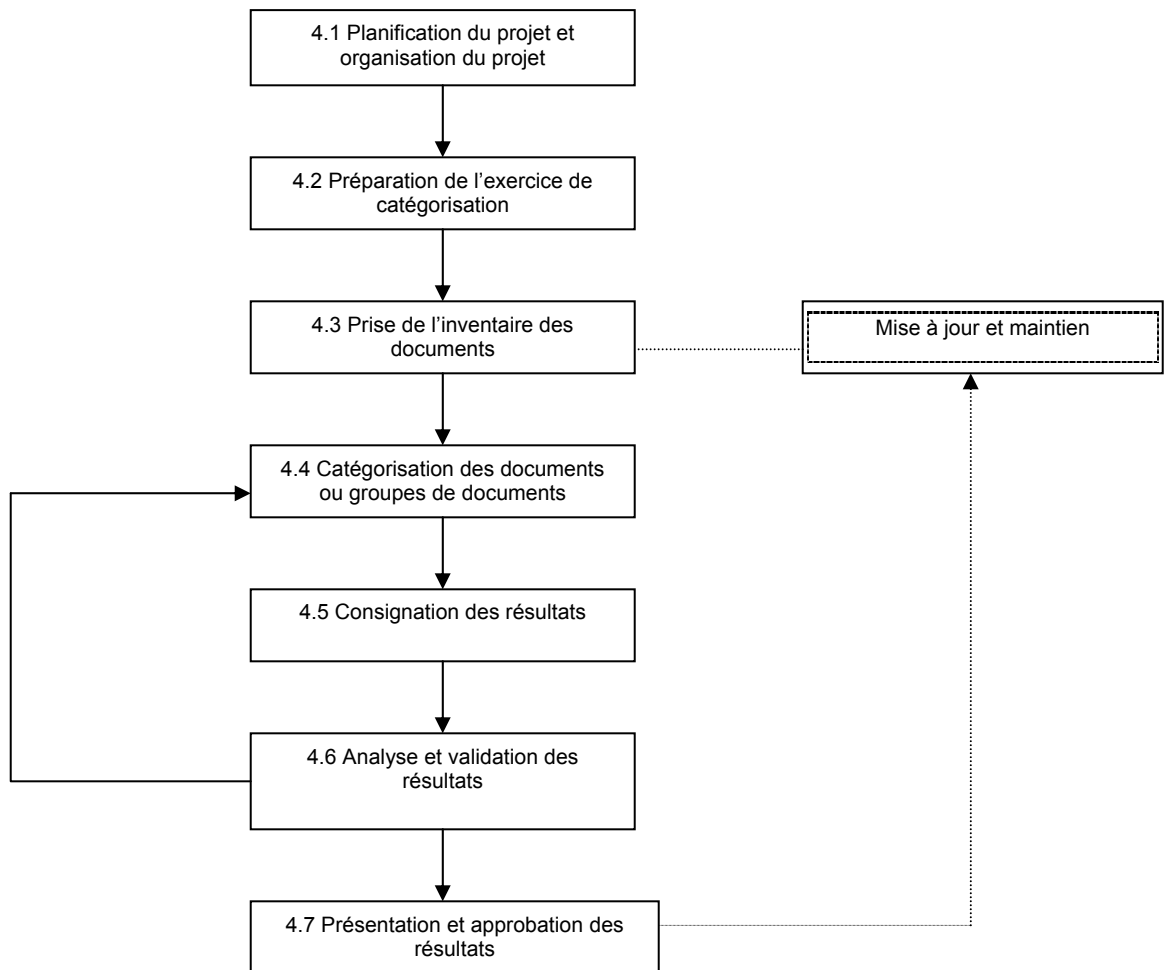


Figure 4 – Étapes du processus de catégorisation

4.1 Planification du projet et organisation du projet

La planification des activités liées au projet de catégorisation et l'organisation du travail sont des éléments importants pour sa réussite. Aux fins de cette planification, une approche de réalisation concrète est proposée ci-dessous, laquelle peut être adaptée et bonifiée selon le contexte et les ressources de chaque établissement.

Il est essentiel de bien circonscrire le niveau de détail selon lequel le processus de catégorisation sera abordé. Une approche visant à demeurer à haut niveau peut constituer un gage de succès parce qu'elle limite :

- Le nombre d'intervenants participant au projet ;
- La durée du projet dans le temps ;
- La quantité de ressources nécessaires ;
- Les efforts nécessaires pour mener le projet à terme.

Les principales activités de planification et d'organisation sont les suivantes :

4.1.1 Réunion du comité de PRP et de sécurité et définition du projet

Cette première étape consiste à réunir le comité de PRP et de sécurité de l'établissement et de définir le projet de catégorisation. Un document de définition de projet est produit.

Au cours de cette étape, le comité de PRP et de sécurité devra suggérer un chargé de projet et l'indiquer dans le document de définition de projet.

4.1.2 Présentation du projet à la direction générale

Le projet devra être présenté à la direction générale par le président du comité de PRP et de sécurité. Le projet devra être approuvé par la direction générale. Cette dernière devra par la suite émettre un communiqué à l'ensemble des gestionnaires des unités administratives qu'un projet de catégorisation est en cours et qu'il exige d'eux leur collaboration.

La direction générale devra au cours de la même réunion approuver la désignation du chargé de projet et lui indiquer formellement cette décision.

4.1.3 Préparation du projet

Le chargé de projet évalue les ressources et les efforts requis et prépare le cahier de projet à cette fin. Il obtient l'approbation et l'engagement de la direction générale. L'ampleur du projet dépendra de différents facteurs, notamment de la disponibilité des informations de base, du niveau de granularité voulu, du nombre de domaines d'activités, du fait que l'établissement soit centralisé ou non, etc.

Un plan de projet sera préparé. Ce plan de projet précise :

1. Les étapes ;
2. Les efforts ;
3. Les ressources ;
4. Le calendrier de réalisation.

La logistique de réalisation du projet doit également être planifiée. À cette fin, les locaux où se dérouleront les rencontres et les moyens pour colliger les informations obtenues seront précisés.

4.1.4 Coordination de l'équipe de projet

Le chargé de projet coordonne la composition de l'équipe de projet, de l'équipe des détenteurs et de l'équipe de collaborateurs (par exemple, en transmettant une lettre aux gestionnaires des unités administratives visées leur expliquant globalement la démarche et leur demandant de désigner une ou quelques personnes clés pour les ateliers).

4.1.5 Réunion de démarrage

L'équipe de projet organise une réunion de démarrage avec les équipes de détenteurs et de collaborateurs. Lors de cette réunion, une formation sur la démarche est fournie aux détenteurs. De plus, une présentation du plan de travail et de l'échéancier ainsi qu'une présentation des rôles de tous les intervenants sont réalisées.

Cette réunion permettra également aux participants, particulièrement les détenteurs de se préparer à l'exercice. À cette fin, on leur demandera de rassembler toutes les informations nécessaires qui permettront de décrire les processus d'affaires de l'établissement. Plus particulièrement, les informations suivantes doivent être préparées par les détenteurs :

1. Les documents utilisés et manipulés dans les différents processus d'affaires ;
2. Le nom des systèmes d'information utilisés en supports ;
3. Le nom des serveurs, le nom de la base de données et la localisation physique du serveur (cette information pourra être obtenue du service informatique) ;
4. Une description narrative ou graphique des processus d'affaires de l'unité administrative, si celle-ci existe ;
5. Des exemples d'écrans de saisie de l'information.

4.2 Préparation de l'exercice de catégorisation

Cette étape consiste principalement pour l'équipe de projet à réunir et à prendre connaissance des documents de préparation.

4.2.1 Recensement des informations et identification des unités administratives

L'équipe de projet recense et examine les informations suivantes si celles-ci sont disponibles :

- Mission et principaux programmes de l'établissement ;
- Objectifs stratégiques ;
- Organigramme de l'organisation ;
- Plan stratégique de l'établissement ;
- Plan stratégique des technologies de l'information ;
- Politique nationale de protection des renseignements personnels du « Cadre global » ;
- Politique de sécurité du « Cadre global » ;
- Politique de confidentialité ;
- Politique d'accès à l'information ;
- Plan de classification ;
- Analyse de risques réalisée antérieurement ;
- Autres documents qui définissent l'établissement.

En consultant l'organigramme, l'équipe de projet détermine quelles sont les unités administratives visées par la catégorisation, selon les domaines d'activités (vice-présidence, direction, service, etc.). Les détenteurs « principaux » sont également identifiés. Un détenteur « principal » est le premier responsable de l'information manipulée dans son unité administrative, que ce soit sous format papier ou électronique.

Pour déterminer l'information à catégoriser, il importe de documenter les processus d'affaires qui contribuent à l'accomplissement de la mission de l'établissement et qui manipulent des actifs informationnels. Il importe aussi de documenter le contexte dans lequel intervient l'établissement car ces facteurs permettent une appréciation des enjeux qui peuvent être rattachés aux actifs informationnels détenus.

Il s'agit d'abord de recensements permettant d'identifier les unités d'affaires qui contribuent à l'accomplissement de la mission et des programmes de l'établissement. Pour ce faire, on peut utiliser l'organigramme de l'établissement comme point de départ. Les principales unités administratives pourront ainsi être facilement cernées car elles découlent habituellement des principales responsabilités et du mandat confié aux différentes directions et services de l'établissement.

Il est important d'identifier les responsables des unités administratives qui sont la plupart du temps les détenteurs des actifs informationnels et qui sont les mieux placés pour identifier l'ensemble de leur processus d'affaires, recenser les documents à l'intérieur des processus et les catégoriser.

Une liste présentant les unités administratives visées et les détenteurs des actifs informationnels devra être préparée. Le tableau 1 présente un exemple de cette liste.

Unité administrative	Détenteur « principal »
Approvisionnement / Installations matérielles	M. Haché
Laboratoire	Mme Locas
Département de médecine générale	Dr Dubois
Médecine / Hospitalisation	Dr Bergeron
Services ambulatoires/Urgence	Mme Ladouceur
Psychiatrie	Mme Binette
Diététique	Mme Lague
Accueil	Mme Leblanc
Radiologie	Mme Corbrau
Comptabilité	M. Vachon
...	...

Tableau 1 : Liste des unités administratives et des détenteurs visés par l'exercice

Généralement, toutes les unités administratives de l'établissement seront visées par cet exercice. Les autres documents permettent de connaître les exigences légales auxquelles est

confronté l'établissement, de même que les orientations actuelles et futures en matière de protection de l'information.

4.2.2 Valider l'étendue de la catégorisation

Cette activité permet de valider la liste des unités administratives, de s'assurer que tous les domaines d'activités sont couverts par l'exercice, de décider que certains de ces domaines ne doivent pas être inclus dans l'exercice de catégorisation et de confirmer l'identification des détenteurs de chacune des unités administratives.

4.2.3 Prise de contact avec les détenteurs

Cette activité est effectuée par le chargé de projet. Elle vise à expliquer aux détenteurs les éléments suivants :

- Les objectifs et la raison d'être de l'exercice de catégorisation.
- Les étapes de catégorisation.
- Leur rôle dans le processus de catégorisation.
- La nécessité de constituer une équipe de travail pour certaines unités administratives qui pourraient être complexes et disposer de plusieurs domaines d'activités. D'autres personnes pourraient se joindre alors au détenteur pour l'aider dans le processus de catégorisation. Cette activité est nécessaire lorsque plusieurs domaines d'activités sont présents pour une même unité administrative. Par exemple, l'unité administrative « Comptabilité » pourrait disposer des domaines d'activités suivants : comptes à payer, paie, comptes à recevoir, écritures comptables. Le détenteur « principal », qui est habituellement le responsable de l'unité administrative, pourrait convoquer ses subalternes responsables de ces domaines d'activités. D'autres part, il peut être possible pour un détenteur « principal » de vouloir être accompagné des principaux utilisateurs des systèmes d'information présents dans son unité administrative.
- Le nombre de rencontres devant être réalisées avec le « détenteur principal ». À cet effet, il faut prévoir les rencontres suivantes :

- **Une rencontre de démarrage et de formation des détenteurs**
- **Une rencontre pour la prise d'inventaire** (étape 4.3 « Prise de l'inventaire des documents ») ;
- **Une rencontre pour l'exercice de catégorisation** (étape 4.4 « Catégorisation des documents ou groupes de documents »)⁴ ;
- **Une rencontre de validation et d'approbation des résultats** (qui pourrait être individuelle ou à l'intérieur d'un comité de validation qui réunirait tous les détenteurs).

Cette activité vise également à s'entendre sur le mode de fonctionnement de l'exercice de catégorisation. Le chargé de projet explique au détenteur « principal » de quelle façon il compte fonctionner pour obtenir la documentation et les informations pertinentes. Il précisera que le mode de fonctionnement habituel sera par atelier de travail.

Le chargé de projet explique également au détenteur « principal » les activités suivantes, soit :

- Le recensement des lois sectorielles ;
- La vérification à l'assujettissement du secteur à des ententes contractuelles ;
- La vérification des directives propres au secteur.

Le chargé de projet précise au détenteur que ces trois dernières activités sont nécessaires afin de permettre à l'équipe de projet ainsi qu'à lui-même d'analyser le contexte de l'établissement, les contraintes administratives ainsi que les exigences légales qui pourraient influencer l'évaluation des seuils d'impact sur le DIC afin de préparer la catégorisation des documents. Le chargé de projet précise que l'aide du détenteur est nécessaire pour que les rencontres de prise d'inventaire et de catégorisation soient productives.

⁴ Selon la complexité de l'unité d'affaires, cette rencontre pourrait être jumelée avec la deuxième rencontre.



Pour ces trois activités, le détenteur et l'équipe de validation peuvent utiliser les documents suivants :

- Site Intranet ou Internet de l'établissement ;
- Formulaires de déclaration de fichiers de renseignements personnels ;
- Cadre global « Volet sécurité » ;
- Cadre global « Volet protection des renseignements personnels » ;
- Lois pertinentes ;
- Calendrier de conservation ;
- Protocoles de recherche ;
- Contrats et ententes commerciales ;
- Plan de classification ;
- Plan de développement de la prestation électronique de services.

Le chargé de projet explique aussi au détenteur :

- Les objectifs et la raison d'être de l'exercice de catégorisation ;
- Les étapes de catégorisation ;
- Le rôle du détenteur :
 1. S'assurer que l'inventaire des actifs informationnels (documents et composantes) est complet
 2. Évaluer les impacts d'une perte de disponibilité, d'intégrité et de confidentialité sur les processus d'affaires dont le détenteur est responsable
 3. Établir une valeur aux actifs en conséquence (selon les trois dimensions de disponibilité, d'intégrité et de confidentialité).

4.2.4. Le recensement des lois sectorielles

Afin d'effectuer cet exercice, l'équipe de projet et le détenteur doivent recenser les lois sectorielles applicables et repérer les dispositions qui peuvent influencer les besoins liés aux objectifs de DIC.

Il s'agit d'abord de recenser les lois et règlements sectoriels applicables à l'établissement. Pour ce faire, l'équipe de projet peut d'abord consulter le site Intranet ou Internet de l'établissement sur lesquels on retrouve habituellement la liste des lois et règlements applicables de même que la mission et les principaux services dispensés.

À la base, les établissements sont régis par la Loi sur les services de santé et de services sociaux⁵ (Lsss) mais l'ensemble de leurs obligations n'est pas encadré par ce seul texte. La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels⁶ (ci-après la Loi sur l'accès) s'applique généralement en ce qui a trait aux documents qui ne font pas partie des dossiers d'utilisateurs. Elle trouve également application dans le cadre de relations avec des entités de droit privé, dans le cadre d'impartition de services par exemple.

La Loi sur la protection des renseignements personnels dans le secteur privé⁷ doit également être considérée.

La Loi sur les archives⁸ confère aux établissements l'obligation de créer un calendrier de conservation des documents et il faut s'assurer que la catégorisation met en oeuvre ces règles.

Les textes relatifs à la protection de la jeunesse⁹ de même que La Loi sur le curateur public, peuvent avoir un impact sur les modalités de traitement et de divulgation d'informations.

La Loi sur la santé publique¹⁰ prévoit des systèmes de surveillance, de communication et de déclarations qui doivent être pris en compte pour s'assurer de la disponibilité des informations nécessaires au respect de la Loi.

⁵ L.R.Q. S-4.2

⁶ L.R.Q. A-2.1

⁷ L.R.Q. P-39.1

⁸ L.R.Q. A-21.1

⁹ La *Loi sur la protection de la jeunesse* (L.R.Q. c. P-34.1) ou la *Loi sur les jeunes contrevenants*, récemment remplacée par la *Loi sur le système de justice pénale pour les adolescents*.

La Loi sur l'assurance-maladie et la Loi sur la Régie de l'assurance maladie du Québec fournissent elles aussi leur ensemble de règles ayant un impact sur la gestion des actifs informationnels des établissements.

Les codes de déontologie des différents professionnels oeuvrant en établissement de même que les principes d'éthique reconnus, doivent être compatibles avec les résultats de la mise en oeuvre des catégorisations.

Ces exemples ne sont évidemment pas limitatifs et une liste des principales lois régissant le secteur de la santé est présentée à l'Annexe 3. L'équipe de projet peut aussi consulter les politiques de l'établissement, plus particulièrement celles sur la protection des renseignements personnels et sur la sécurité de l'information, qui contiennent généralement une section décrivant le cadre législatif et réglementaire spécifique de l'établissement. Elle peut également, au besoin, organiser une rencontre avec le conseiller juridique de l'établissement pour valider certains aspects.

Il s'agit de rechercher les dispositions légales qui touchent les documents de l'établissement, y compris les exigences qui concernent des documents sur support papier.

On recherchera plus particulièrement les dispositions légales qui :

- Tiennent compte des exigences de confidentialité des renseignements personnels et des documents détenus par l'établissement. Par exemple, plusieurs lois contiennent des dispositions dérogatoires à la Loi sur l'accès qui confèrent un caractère confidentiel à des documents qui seraient normalement considérés comme publics¹¹.
- Prévoient des exigences particulières en ce qui a trait à la disponibilité des services offerts de manière électronique ou des documents (par exemple, la disponibilité des registres publics informatisés, services essentiels, etc.).
- Prévoient des exigences particulières en matière d'irrévocabilité et d'intégrité des documents. Par exemple, on peut considérer si :

¹⁰ L.R.Q. S-2.2. D'autres textes connexes seraient à consulter: la *Loi sur les laboratoires médicaux, la conservation des organes, des tissus, des gamètes et des embryons et la disposition des cadavres*, L.R.Q. I-0.2, et la *Loi sur les services préhospitaliers d'urgence*, L.R.Q. S-6.2.

- Les textes constitutifs de l'établissement prévoient, font référence ou sont assujettis à des dispositions spécifiques quant au pouvoir de signature de certains actes juridiques ou administratifs d'importance qui sont conclus de manière électronique par l'établissement.
- L'établissement est appelé à produire ou à maintenir des documents authentiques ou des copies certifiées conformes officielles sur support électronique (registres publics, certificats officiels, etc.).
- Les activités de l'établissement entraînent la conclusion de contrats ou d'actes de manière électronique qui doivent respecter des formalités particulières prévues par le Code civil du Québec (actes authentiques, actes sous seing privé, etc.).

Ces éléments d'information influenceront l'évaluation des impacts sur le DIC et guideront l'établissement au moment de la sélection des mécanismes de sécurité à mettre en place, tels que la journalisation, l'authentification, la signature numérique, la notariation, etc.

4.2.5 La vérification à l'assujettissement du secteur à des ententes contractuelles

Afin d'effectuer cet exercice, l'équipe de projet, de concert avec le détenteur, doit vérifier si l'établissement est assujetti à des ententes contractuelles ou administratives qui prévoient des obligations particulières en matière de PRP et de DIC.

Cette tâche consiste à vérifier si l'établissement est assujetti à des obligations particulières en vertu d'ententes contractuelles ou administratives conclues avec d'autres établissements, ministères, ou encore avec des tiers, et qui peuvent influencer l'évaluation des seuils d'impact sur le DIC.

Par exemple, il faudra notamment vérifier les ententes telles que :

- Les ententes relatives aux activités de recherche ;
- Les ententes d'échange ou de transfert de renseignements personnels ;

¹¹ On peut notamment consulter l'ouvrage intitulé *Accès à l'information - Loi annotée, jurisprudence, analyse et commentaires*, Doray, Raymond et Charrette, François, Yvon Blais, 2002.

- Les ententes pour la réalisation de sondages ;
- Les projets pilotes comportant des traitements d'informations sensibles ;
- Les ententes de service ou conventions d'impartition relatives à la gestion des ressources humaines, matérielles et financières ;
- Les ententes de service relatives à l'exploitation et à la maintenance des systèmes d'information, notamment celles découlant de l'offre de service commun de l'infrastructure gouvernementale (Infrastructure à clé publique gouvernementale, Répertoire, Registres, etc.) ;
- Les ententes de sécurité pour les échanges avec d'autres domaines de confiance (AGSIN) ;
- Les ententes de services professionnels interétablissements ;
- Les ententes de services avec des professionnels du secteur privé ;
- Etc.

4.2.6. La vérification des directives propres au secteur

Cette tâche consiste à vérifier si l'établissement a émis des directives spécifiques concernant les exigences de PRP et de sécurité de certains types de documents, en fonction de leur structure logique ou de leur nature.

Par exemple, l'établissement peut avoir formulé une directive sur les exigences de PRP et de sécurité applicables aux renseignements personnels sur la clientèle. Il peut également avoir formulé une directive semblable pour la gestion de ses formulaires électroniques ou autres documents ayant une structure logique commune.

4.3 Prise de l'inventaire des documents

4.3.1 Les fondements

Cette étape consiste à inventorier les informations détenues ou utilisées par les établissements pour leur propre compte ou celui d'un tiers, tant au niveau des documents, des dépôts d'information que des flux de communication ou de transferts de ces informations. Cette étape consiste donc à identifier, pour chaque unité administrative :

- Le ou les principaux processus d'affaires permettant à l'unité administrative de réaliser sa mission ;
- Le ou les systèmes d'information qui supportent les processus d'affaires identifiés;
- Le ou les domaines d'activités ;
- Le ou les types de documents sous format papier ou technologique qui sont emmagasinés, générés, traités ou échangés ;
- Les systèmes d'information qui contiennent des renseignements personnels.



Il est important à cette étape de comprendre la notion de document.

La notion de document s'entend d'un objet constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcritibles sous l'une de ces formes ou en un autre système de symboles. Par exemple, le braille est un système de symboles transcritibles. C'est en ce sens que l'on peut parler des actifs informationnels comme regroupement de documents.

La notion de document utilisée ici postule que tous les documents ont une structure commune. Les supports peuvent donc être interchangeable mais le document lui, demeure toujours un ensemble d'informations délimité et structuré de façon tangible et logique sous forme de mots, de sons ou d'images.



Le concept de document technologique est défini par la *Loi concernant le cadre juridique des technologies de l'information*. On peut le définir comme suit :

Document technologique : Une information délimitée et structurée de façon logique sur un support faisant appel aux technologies de l'information, intelligible sous forme de mots, de sons ou d'images. Est assimilée au document technologique toute banque de données dont les éléments structurants permettent la création de documents par la délimitation ou la structuration de l'information qui y est inscrite.

L'utilisation du formulaire, présenté au tableau 2, est recommandée. L'équipe de projet, avec le détenteur, identifie les documents ou groupe de documents et consigne ces informations sur un formulaire prévu à cette fin. Il est important d'utiliser un formulaire différent pour chaque document ou groupe de documents.

Si un document peut être à la fois papier et électronique, il faut l'indiquer sur la fiche car les niveaux de sensibilité peuvent être différents pour chaque document.

Le détenteur doit bien comprendre la nature d'un document. Le chargé de projet (ou l'équipe de projet) doit lui rappeler la définition d'un document (voir l'encadré ci-dessus).

Le **tableau 2** présente le format du formulaire devant être utilisé.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

<input type="checkbox"/> FORMULAIRE D'INVENTAIRE ET DE CATÉGORISATION							
Partie A : INVENTAIRE							
Nom de l'unité administrative :				Nom du détenteur :			
Nom du processus d'affaires :				Gestion centralisée/décentralisée de la sécurité logique :			
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom des systèmes d'information supportant le processus :				Nom des composantes de support		Localisation	
<u>Localisation des documents physiques</u>							
Nom du document ou groupe de documents			Description des mécanismes de rangements				
<u>Alimentation d'un autre processus (système ou document)</u>				Alimentation vers un autre processus			
Nom du processus (système ou document) :				Nom du processus :			
Catégorisation du processus :	D	I	C	Commentaires	Moyen de transmission :		
					Commentaires :		
Moyens de transmission :							
Partie B: CATÉGORISATION							
CRITÈRES	CATÉGORISATION				EXPLICATIONS/EXIGENCES SPÉCIFIQUES		
	Bas ----->Très élevé						
DISPONIBILITÉ	1	2	3	4			
INTÉGRITÉ	1	2	3	4			
CONFIDENTIALITÉ	1	2	3	4			

Tableau 2 : Formulaire/partie A : Prise d'inventaire

Les éléments à remplir sont les suivants :

- Le nom de l'unité administrative ;
- Le nom du détenteur ;
- Le nom du processus d'affaires. Une unité administrative peut avoir plusieurs processus d'affaires pour accomplir sa mission. Par exemple, le service de la pharmacie peut disposer des processus suivants : ;
 1. Traitement des prescriptions
 2. Inventaire et commande des médicaments
 3. Gestion interne du service
- La gestion de la sécurité logique est-elle centralisée ou décentralisée? La réponse à cette question permettra de planifier l'intervention lors de l'évaluation de la situation actuelle de l'établissement ;
- Le nom de chacun des documents à catégoriser. Ces documents sont identifier en effectuant la description de chacun des processus et en faisant l'inventaire des documents ou groupes de documents manipulés à l'intérieur du processus;
- Le format du document (papier ou électronique) ;
- La présence de PRP à l'intérieur du document ;
- Le fait que le document est inscrit ou non au calendrier de conservation ;
- Le système d'information utilisé pour manipuler ou conserver l'information sur le document, ainsi que le support du système (serveur, système d'exploitation, base de données). La localisation du serveur devrait être mentionnée. Ces informations peuvent être obtenues par le service informatique. Habituellement, on retrouve un système d'information par processus. Mais il peut arriver que deux ou plusieurs systèmes soient utilisés pour un processus ;

- Si le processus d'affaires est alimenté par un autre processus d'affaires (habituellement un système d'information), il est important de l'identifier et d'obtenir sa cote de catégorisation de la part du propriétaire ;
- Si le processus étudié alimente un autre processus, il est important de les recenser.



À quel niveau de granularité doit-on recenser les groupes de documents ?

Compte tenu que l'objectif de la catégorisation est de déterminer globalement les besoins de PRP et de sécurité afin d'établir la base permettant d'évaluer les risques, il n'est pas nécessaire de recenser tous les documents mais uniquement ceux pour lesquels une atteinte aurait des impacts négatifs et qui ont pour les établissements une valeur, que celle-ci soit administrative, légale, patrimoniale ou économique. En fait, un regroupement à haut niveau des groupes de documents est fortement recommandé pour simplifier l'exercice de catégorisation. Pour ce faire, les documents de même nature ou comportant des caractéristiques similaires pourront être regroupés.



Par exemple :

- Le dossier usager serait le groupe de documents regroupant les informations sur un usager;
- Le dossier d'employé regrouperait les informations sur les employés et pourrait être papier ou électronique.

4.3.2 Les techniques de documentation des processus d'affaires

La prise d'inventaire des documents devrait se faire pour chaque processus d'affaires de l'unité administrative. Un processus d'affaires est constitué d'une série d'étapes et a un début et une fin d'activité. Le processus d'affaires contribue à la mission de l'unité administrative.

Une façon simple d'identifier les documents papier et électronique utilisés ou manipulés à l'intérieur d'un processus d'affaires consiste à décrire le processus du début à la fin de son cycle.

La figure 5 illustre une façon graphique de documenter un processus

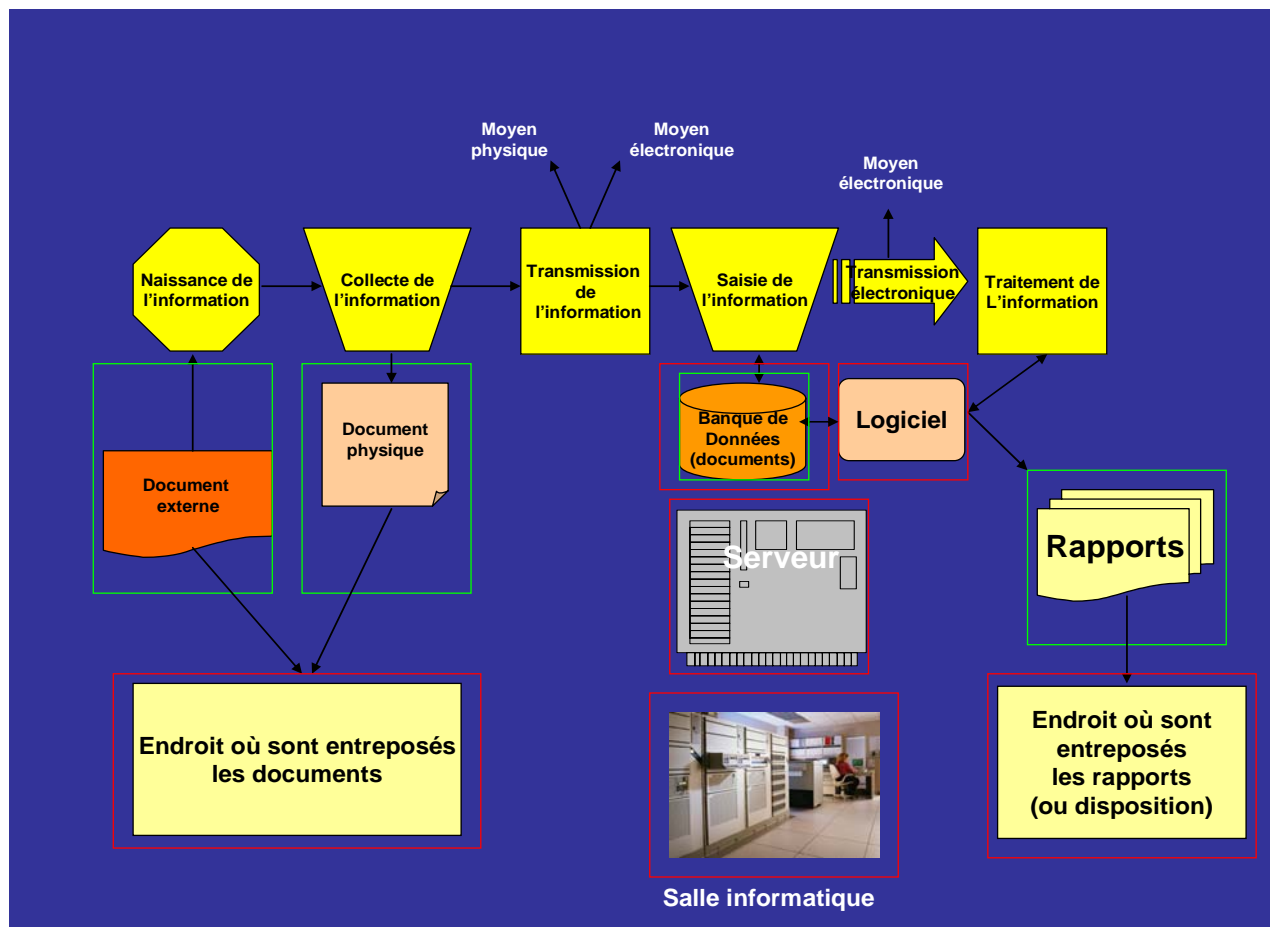


Figure 5 : Exemple de documentation de processus

Le recensement des documents et des composantes de support doit être fait en comprenant bien les activités liées au processus. La plupart des processus ont une « chaîne de traitement ». Par exemple :

- Naissance de l'information
- Collecte de l'information sur un document papier
- Transmission physique et manipulation du document
- Saisie du document
- Transmission électronique du document
- Traitement de l'information
- Entreposage électronique des résultats du traitement
- Sortie des résultats et manipulation des rapports
- Entreposage des rapports (ou disposition)
- Destruction de l'information

4.3.3 Exemple d'application

L'exemple suivant illustre le processus de prise d'inventaire :

Une prescription d'un médecin qui a été préparée sur format papier. Elle est saisie dans le système d'information de pharmacie. L'équipe de projet demande au service informatique le nom du serveur sur lequel réside le système. Elle demande également si des liens sont présents avec d'autres systèmes.

Le formulaire présenté au **tableau 3** illustre les informations remplies par l'équipe de projet.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

<input type="checkbox"/> FORMULAIRE D'INVENTAIRE ET DE CATÉGORISATION						
Partie A : INVENTAIRE						
Nom de l'unité administrative : Service de laboratoire			Nom du détenteur : Maude Lemay			
Nom du processus d'affaires : Requête résultats			Gestion centralisée/décentralisée de la sécurité logique : Centralisée			
Nom du document : Requête-papier	D	I	C	Papier : <input checked="" type="checkbox"/> Électronique : <input type="checkbox"/>	Présence de PRP? OUI	Inscrit au calendrier de conservation : N
Nom du document : Requête-saisie	D	I	C	Papier : <input type="checkbox"/> Électronique : <input checked="" type="checkbox"/>	Présence de PRP? OUI	Inscrit au calendrier de conservation : N
Nom du document : Requête résultats-enregistrement	D	I	C	Papier : <input type="checkbox"/> Électronique : <input checked="" type="checkbox"/>	Présence de PRP? OUI	Inscrit au calendrier de conservation : N
Nom du document : Requête résultats-imprimée	D	I	C	Papier : <input checked="" type="checkbox"/> Électronique : <input type="checkbox"/>	Présence de PRP? OUI	Inscrit au calendrier de conservation : N
Nom du document :	D	I	C	Papier : <input type="checkbox"/> Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom des systèmes d'information supportant le processus :			Nom des composantes de support		Localisation	
SoftLab			Oracle-Unix Serveur UX01		Salle informatique du pavillon principal	
Localisation des documents physiques						
Nom du document ou groupe de documents			Description des mécanismes de rangements			
Requêtes et résultats imprimés			Classeur situé dans le laboratoire			
Alimentation d'un autre processus (système ou document)				Alimentation vers un autre processus		
Nom du processus (système ou document) : Index-Patient (coordonnées du patient)				Nom du processus :		
Catégorisation du processus :	D	I	C	Moyen de transmission :		
	3	4	3	Commentaires :		
Moyens de transmission : Réseau de télécommunication						
Partie B: CATÉGORISATION						
CRITÈRES	CATÉGORISATION				EXPLICATIONS/EXIGENCES SPÉCIFIQUES	
	Bas ----->Très élevé					
DISPONIBILITÉ	1	2	3	4		
INTÉGRITÉ	1	2	3	4		
CONFIDENTIALITÉ	1	2	3	4		

Tableau 3 : Prise d'inventaire des documents



Il est important de déterminer si le document provient d'un processus d'affaires et/ou si le document est également transféré vers d'autres processus d'affaires car la valeur de catégorisation du document pourrait être héritée de l'évaluation faite en amont.

De même, le fait de transférer le document à un autre système peut signifier que la valeur de catégorisation sera également la même à l'intérieur de l'autre système.

Il faudra ainsi tenir compte de ces informations dans le processus de catégorisation expliqué ultérieurement.



Il est également important d'obtenir les informations relatives à l'environnement technologique supportant le processus d'affaires car les mesures de protection du document sont liées aux mesures de protection de l'infrastructure (le système d'exploitation, la base de données, la localisation physique du serveur, etc.).

Une unité d'affaires peut être découpée en plusieurs processus d'affaires. Par exemple, l'unité administrative « Ressources Humaines » peut être constituée des processus suivants :

1. Dotation et embauche
2. Rémunération
3. Communication aux employés
4. Évaluation et rendement
5. Départ



Il est important de limiter le nombre de processus d'affaires pour une même unité administrative afin de conserver un degré de simplicité. Ainsi, une règle pourrait limiter le nombre de processus d'affaires entre 2 et 6. Des regroupements pourraient être alors nécessaires.



Il est important de déterminer si le document provient d'autres systèmes d'information et/ou si le document est également transféré vers d'autres systèmes d'information, car la valeur de catégorisation du document pourrait être héritée de l'évaluation faite en amont.

De même, le fait de transférer le document à un autre système peut signifier que la valeur de catégorisation sera également la même à l'intérieur de l'autre système.

Il faudra ainsi en tenir compte dans le processus de catégorisation expliqué ultérieurement.



Il est important également de préciser le nom du serveur car le choix des mesures de protection du document passera également par la protection de l'infrastructure qui supporte le document, tels les bases de données, le système d'exploitation, etc.



La prise d'inventaire des documents devrait se faire pour chaque processus d'affaires de l'unité administrative. Un processus d'affaires est constitué d'une série d'étapes et a un début et une fin d'activité. Le processus d'affaires contribue à la mission de l'unité administrative.



Pour le chargé de projet, il ne s'agit pas de décrire formellement le processus d'affaires. Cette tâche appartient au détenteur et elle va au-delà des activités nécessaires pour la catégorisation. Il s'agit uniquement à travers une description de haut niveau mais informelle d'identifier les documents utilisés pour réaliser les activités du processus.



Pour le chargé de projet, il ne s'agit pas de décrire formellement le processus d'affaires. Cette tâche appartient au détenteur et elle va au-delà des activités nécessaires pour la catégorisation. Il s'agit uniquement à travers une description de haut niveau mais informelle d'identifier les documents utilisés pour réaliser les activités du processus.



Le recensement des documents et des composantes de support doit être fait en comprenant bien les activités liées au processus. La plupart des processus ont une « chaîne de traitement ». Par exemple :

- Naissance de l'information ;
- Collecte de l'information sur un document papier ;
- Transmission physique et manipulation du document ;
- Saisie du document ;
- Transmission électronique du document ;
- Traitement de l'information ;
- Entreposage électronique des résultats du traitement ;
- Sortie des résultats et manipulation des rapports ;
- Entreposage des rapports (ou disposition) ;
- Destruction de l'information.

On remarque que l'inventaire des documents tient compte également des composantes qui les soutiennent tant au niveau physique qu'au niveau électronique. En effet, le processus de catégorisation permet d'identifier les documents physiques et électroniques qui sont importants ou non pour l'établissement. Ainsi, si un document papier est important, ses composantes sont également importantes; il faudra déterminer où se trouve le document (classeur, local) pour ensuite effectuer une analyse de risques sur ces composantes et revoir les mécanismes de protection des composantes qui soutiennent le document physique. Dans le même ordre d'idée, si un document électronique devient important :

- La base de données qui contient le document devient importante ;
- Le logiciel d'application devient important ;
- Le serveur et le logiciel d'exploitation deviennent importants ;
- La localisation physique où se trouve le serveur devient importante.

L'analyse de risques sera faite sur chaque composante supportant le document électronique.

4.4 Catégorisation des documents ou groupes de documents

4.4.1 Préparation à l'exercice

Les documents à catégoriser font l'objet d'une évaluation des impacts advenant un manque de disponibilité, d'intégrité et de confidentialité. Cette étape permet de déterminer le seuil de tolérance à ces risques. Il s'agit ensuite d'assigner à chaque document un seuil d'impact « très élevé », « élevé », « moyen » ou « bas » pour chacune des dimensions du DIC. Ces seuils d'impact sont expliqués à la section 4.4.3.

À cette fin, la partie du bas du « Formulaire d'inventaire et de classification », qui sert à l'inventaire des documents, est utilisée.



Tout au long de l'étape de catégorisation, il est important :

- De se rappeler que les documents papiers et électroniques seront catégorisés de l'importance des informations consignées sur ces derniers;
- De bien définir le niveau de détail selon lequel le processus de catégorisation sera abordé; une approche visant à demeurer à haut niveau peut constituer un gage de succès;
- De prendre en considération que le même document, papier et électronique, peut être catégorisé différemment.



Il est fortement recommandé d'effectuer la catégorisation de l'information en collaboration avec les responsables de la gestion des documents ainsi que le responsable de la protection des renseignements personnels et de l'accès à l'information de l'établissement.

Les établissements pourront alors établir les mesures à mettre en place parmi celles qui sont généralement appliquées, compte tenu du contexte d'utilisation et des valeurs attribuées à leurs attributs.

Un domaine d'activités peut, au cours de son cycle de vie, avoir un niveau de confidentialité élevé pour une période donnée et être public pour une autre période. Normalement, la catégorisation doit être revue au cours du cycle de vie. Autrement, on attribue la valeur la plus élevée de son cycle de vie.



Tout **au long de cette étape de catégorisation**, il est important :

- De se rappeler que les actifs informatiques seront catégorisés en fonction des informations, banques de données et autres qu'ils supportent ;
- De bien définir le niveau de détails selon lequel le processus de catégorisation sera abordé; une approche visant à demeurer à haut niveau peut constituer un gage de succès ;
- De prendre en considération que le même document, papier et électronique, peut être catégorisé différemment.



Il est fortement recommandé d'effectuer la catégorisation de l'information en collaboration avec les responsables de la gestion des documents ainsi que le responsable de la protection des renseignements personnels et de l'accès à l'information de leur établissement.

4.4.2 Le processus de catégorisation

À l'aide de la définition des seuils d'impact et du cycle de vie des documents, l'équipe de projet et le détenteur attribuent une valeur à ces derniers en fonction des impacts pour *l'établissement* d'une perte de DIC. À cette fin, une évaluation individuelle des documents recensés et consignés dans la fiche de prise d'inventaire est effectuée. Par la suite, une cote globale est attribuée à **l'ensemble du processus d'affaires** en tenant compte des valeurs les plus élevées accordées à chaque document ou groupe de documents.

L'évaluation des impacts d'une perte de DIC pour un document s'effectue par rapport à la mission et aux objectifs d'affaires de l'établissement et du rôle du processus d'affaires face à la mission et aux objectifs d'affaires de l'établissement. Il importe de se recentrer fréquemment sur cette perspective.

4.4.3 Définition et explications des seuils d'impact

La grille qui suit fournit des indications quant à certains types d'information et à la façon dont ils peuvent se voir concernés par une atteinte à l'un des attributs du DIC. Au moment de la détermination des seuils d'impact, il peut être utile de considérer si les manques de disponibilité, d'intégrité ou de confidentialité peuvent entraîner des conséquences telles que :

- Incapacité de l'établissement à remplir sa mission ;
- Infraction ou manquement aux lois, aux règlements ou à d'autres normes applicables ;
- Atteinte à la vie privée ;
- Perte d'image ou dommage à la réputation ;
- Perte de confiance de la clientèle ;
- Perturbation des activités de l'établissement ;
- Impossibilité de remplir ses obligations contractuelles ;
- Pertes financières, augmentation des coûts ;

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

- Atteinte à la santé et/ou à la sécurité de la clientèle, du personnel, des partenaires ;
- Dommages moraux ou matériels ;
- Perte de connaissances techniques, de procédés, de savoir-faire ;
- Poursuites éventuelles ;
- Etc.

Pour chaque élément, il est convenu que les niveaux de chaque attribut suivront l'échelle présentée au tableau 4:

Niveau 1	<p>Bas : Impact non significatif</p> <p>Incidences minimales limitées à un secteur administratif de l'établissement sans conséquences pour des tiers.</p>	<p>Incidences d'ordre administratif circonscrites et traitées localement sans affecter l'établissement sur le plan global. La mission est réalisée et aucun impact sur l'image, la réputation, etc.</p> <p>Pas d'impact médical. Toutefois, impact négligeable sur le plan financier.</p>
Niveau 2	<p>Moyen : Impact limité</p> <p>Incidences notables mais limitées à un secteur administratif de l'établissement bien que pouvant avoir des conséquences mineures pour des tiers.</p>	<p>Incidences notables d'une durée limitée sur l'image, le fonctionnement global ou les opérations d'un secteur de l'établissement.</p> <p>L'impact peut se résorber facilement et rapidement. Impact mineur sur les plans médical ou financier. Aucun dommage important à des tiers, ne représente pas un manquement aux obligations médicales ou légales de l'établissement.</p>
Niveau 3	<p>Élevé : Impact grave</p> <p>Incidences notables pour l'établissement ou des tiers mais ne menaçant pas la continuité de l'établissement ou de ses services, mais pouvant avoir des conséquences pour la santé ou la sécurité de personnes physiques.</p>	<p>L'événement aurait des incidences sérieuses et pourrait être la cause de dommages sérieux à des tiers ou nuire aux opérations critiques.</p> <p>La vie de personnes ou la continuité des activités de l'établissement ne sont pas en péril.</p> <p>Impact sérieux sur les plans médical et/ou financier et peut constituer un manquement aux obligations médicales et/ou juridiques. On peut notamment penser aux questions de protection de la vie privée.</p>
Niveau 4	<p>Très élevé : Impact extrêmement grave</p> <p>Incidences très graves menaçant la continuité de l'établissement. Conséquences très sérieuses pour la santé ou la sécurité de personnes physiques.</p>	<p>Incidences extrêmement sérieuses pour l'établissement, des individus ou d'autres entités externes.</p> <p>La santé ou la sécurité de personnes pourraient être mises en péril. Le fonctionnement et les opérations critiques de l'établissement ou d'autres établissements pourraient être paralysés ou compromis. Les conséquences sur le plan humain ou financier peuvent être désastreuses.</p>

Tableau 4 : Définition des seuils d'impact

L'**annexe 1** présente une définition détaillée des seuils d'impact pour chacun des objectifs du DIC et fournit des exemples appropriés. Il est important pour l'équipe de projet de bien maîtriser le contenu de cette annexe et d'y référer constamment lors de l'exercice de catégorisation.

4.4.4 Évaluer les seuils d'impact

L'équipe de projet ainsi que le détenteur utilisent à cette fin le formulaire prévu à cette fin en complétant la partie pour chaque document recensé et en complétant également la partie du bas, une fois les évaluations individuelles des documents réalisées. L'équipe de projet se réfère aux définitions détaillées et aux exemples présentés à l'**annexe 1**. À l'aide de la définition des seuils d'impact, on attribue une valeur aux attributs du DIC pour chaque document ou groupe de documents visés. La valeur globale du processus d'affaires prendra la valeur la plus élevée de chacune des dimensions du DIC.



Par exemple, si nous retrouvons trois documents pour un processus d'affaires. L'évaluation individuelle des seuils d'impacts démontre que :

- Le premier document a une évaluation de 2 pour la Disponibilité, 3 pour l'intégrité et 4 pour la confidentialité;
- Le second document a une évaluation de 3 pour la Disponibilité, 2 pour l'Intégrité et 3 pour la Confidentialité;
- Le troisième document a une évaluation de 2 pour la Disponibilité, 2 pour l'Intégrité et 2 pour la Confidentialité

L'évaluation globale du processus prendra la plus grande valeur rencontrée pour chaque document soit : 3 pour D, 3 pour I et 3 pour C. Comme nous le verrons plus loin, le 3^e document n'a pas une grande importance, son évaluation étant de 2 globalement.

4.4.5 Formulaire utilisé

Le « Formulaire d'inventaire et de catégorisation », déjà utilisé pour effectuer l'inventaire des documents et groupes de documents, est également utilisé pour réaliser la catégorisation de chacun des documents. Le tableau 5 présente la partie B « Catégorisation du processus » à la page suivante.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

<input type="checkbox"/> FORMULAIRE D'INVENTAIRE ET DE CATÉGORISATION							
Partie A : INVENTAIRE							
Nom de l'unité administrative :			Nom du détenteur :				
Nom du processus d'affaires :			Gestion centralisée/décentralisée de la sécurité logique :				
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom des systèmes d'information supportant le processus :			Nom des composantes de support		Localisation		
<u>Localisation des documents physiques</u>							
Nom du document ou groupe de documents		Description des mécanismes de rangements					
<u>Alimentation d'un autre processus (système ou document)</u>				Alimentation vers un autre processus			
Nom du processus (système ou document) :				Nom du processus :			
Catégorisation du processus :	D	I	C	Commentaires		Moyen de transmission :	
						Commentaires :	
Moyens de transmission :							
Partie B: CATÉGORISATION							
CRITÈRES	CATÉGORISATION				EXPLICATIONS/EXIGENCES SPÉCIFIQUES		
	Bas ----->Très élevé						
DISPONIBILITÉ	1	2	3	4			
INTÉGRITÉ	1	2	3	4			
CONFIDENTIALITÉ	1	2	3	4			

Tableau 5 : Formulaire d'inventaire et de catégorisation (partie B)

4.4.6 Exemple d'application

Le scénario précédent, utilisé à la section 4.3.2, est repris dans le présent exemple. Le tableau 6 démontre l'exercice de catégorisation.



L'équipe de projet a complété le formulaire en compagnie du détenteur « principal » ou de l'équipe de détenteurs. Ils se sont référés, pour chacun des éléments du DIC, à la définition des seuils d'impact présentés au tableau 5 « Définition des seuils d'impact ». Ils ont également consulté l'annexe 1 pour appliquer ces seuils d'impact à chacun des objectifs du DIC.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

<input type="checkbox"/> FORMULAIRE D'INVENTAIRE ET DE CATÉGORISATION							
Partie A : INVENTAIRE							
Nom de l'unité administrative : Service de pharmacie				Nom du détenteur : Johanne Vincent			
Nom du processus d'affaires : Prescription				Gestion centralisée/décentralisée de la sécurité logique : Décentralisée			
Nom du document : Prescription papier	D	I	C	Papier : <input checked="" type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP? OUI	Inscrit au calendrier de conservation : N
	1	4	3				
Nom du document : Prescription saisie	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input checked="" type="checkbox"/>	Présence de PRP? OUI	Inscrit au calendrier de conservation : N
	3	4	3				
Nom du document : Liste des ordonnances	D	I	C	Papier : <input checked="" type="checkbox"/>	Électronique : <input checked="" type="checkbox"/>	Présence de PRP? OUI	Inscrit au calendrier de conservation :N
	3	4	3				
Nom du document : Étiquettes	D	I	C	Papier : <input checked="" type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP? OUI	Inscrit au calendrier de conservation : N
	3	4	3				
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP?	Inscrit au calendrier de conservation :
Nom des systèmes d'information supportant le processus :				Nom des composantes de support		Localisation	
CGSI				Oracle-NTserveur NT10		Salle informatique du pavillon principal	
Localisation des documents physiques							
Nom du document ou groupe de documents			Description des mécanismes de rangements				
Prescriptions papiers			Copie dans le classeur dans le local de pharmacie/copie dans le dossier patient				
Alimentation d'un autre processus (système ou document)				Alimentation vers un autre processus			
Nom du processus (système ou document) : Index-Patient (coordonnées du patient)				Nom du processus :			
Catégorisation du processus :	D	I	C	Commentaires		Moyen de transmission :	
	3	4	3			Commentaires :	
Moyens de transmission : Réseau de télécommunication							
Partie B: CATÉGORISATION							
CRITÈRES	CATÉGORISATION				EXPLICATIONS/EXIGENCES SPÉCIFIQUES		
	Bas -----►Très élevé						
DISPONIBILITÉ	1	2	3	4			
INTÉGRITÉ	1	2	3	4			
CONFIDENTIALITÉ	1	2	3	4			

Tableau 6 : Partie B du formulaire permettant la catégorisation



L'exercice de catégorisation se fait pour l'ensemble du processus « Prescription ». Il s'agit de déterminer les impacts sur l'établissement d'une perte de :

- Disponibilité (plus critique si le processus est informatisé)
- Intégrité
- Confidentialité

Comme on le remarque, l'évaluation se fait individuellement pour chaque document. Par la suite, une cote globale est attribuée au processus d'affaires en fonction des cotes individuelles.

4.5 Consignation des résultats

4.5.1 Critères de sélection

Cette étape consiste pour l'équipe de projet à réunir sous un même document intitulé « Matrice de catégorisation » l'ensemble des formulaires utilisés et à pouvoir synthétiser l'ensemble des analyses de catégorisation pour tous les documents de l'établissement. Le tableau 7 présente la matrice de catégorisation.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

Unité administrative	Processus d'affaires	Détenteur	Documents ou groupes de documents	Systèmes d'information	Localisation (serveurs/composantes)	Intrant/Extrant	Gestion centralisée (O ou N)	Type de document (P ou E)	Seuils d'impact			Document sélectionné	Date de création/MAJ
									D	I	C		

Tableau 7 : Matrice de catégorisation

Cette matrice présente une vue d'ensemble des documents qui ont été catégorisés.

La consignation des résultats permet de voir, pour chaque document, les cotes attribuées. Il s'agit maintenant d'identifier ceux qui seront sélectionnés pour l'analyse de risques.

La sélection des documents, qui seront utilisés pour une analyse de risques, a comme critère de ne retenir que ceux dont la cote est de 3 ou 4, dans au moins un des objectifs du DIC. À cette fin, la colonne « document sélectionné » précise les documents effectivement sélectionnés.



Pour être plus clair, il se peut que le dossier usager (qui est un document) soit utilisé par deux unités administratives ou qu'il soit présent dans deux systèmes différents. Par exemple, un système peut maintenir le dossier usager (mise à jour) et les données de ce même dossier peuvent être déversées dans un autre système (un entrepôt de données par exemple). Deux évaluations peuvent alors en ressortir :

- L'unité administrative A peut évaluer le dossier usager selon ses propres besoins ou critères de DIC alors que l'unité administrative B peut l'évaluer selon d'autres besoins ou critères de DIC :

Unité	Document	D	I	C
A	Dossier usager	2	3	3
B	Dossier usager	4	2	3

- Le système 1 peut être évalué différemment du système 2 :

Unité	Système	Document	D	I	C
X	1	Dossier usager	3	2	3
Y	2	Dossier usager	2	4	3

Ainsi, la sélection des documents pourrait être différente selon l'unité administrative. Les zones ombragées indiquent que le document est retenu pour fin de catégorisation.

4.5.2 Exemple d'application

L'exemple suivant (tableau 8) illustre les concepts de sélection des documents. Les renseignements consignés sur cette matrice proviennent de chacun des formulaires utilisés. Comme nous pouvons le remarquer, la colonne « document sélectionné » permet d'indiquer que le document a été retenu pour fin d'analyse de risques, puisqu'au moins un des trois attributs (disponibilité, confidentialité ou intégrité) obtient la valeur 3 ou 4, tel qu'il est précisé dans la section précédente. On indique par un « oui » si le document a été sélectionné pour fin de catégorisation. Par contre, si ce document provient d'un autre système d'information, il faut s'assurer que les cotes accordées au document sont au moins aussi élevées que celles accordées pour le document provenant de ce système.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

Unité administrative	Processus d'affaires	Détenteur	Documents ou groupes de documents	Systèmes d'information	Localisation (serveurs/ composants)	Intrant	Extrant	Gestion centralisée (O ou N)	Type de document (P ou E)	Seuils d'impact			Processus sélectionné	Date de création/MAJ
										D	I	C		
Pharmacie	Prescriptions	Robinson	Prescriptions						P	3	4	3	OUI	
Pharmacie	Prescriptions	Robinson	Prescriptions	CGSI	UX-04/Salle info	Index/patient	Chart-maxx	OUI	E	3	4	3	OUI	
Pharmacie	Prescriptions	Cote globale du processus								3	4	3		
Approvisionnement	Achats	Haché	Bons de Commande	Maestro	NT-U01/Salle info		SAP	NON	E	2	2	2	NON	
Approvisionnement	Achats	Cote globale du processus								2	2	2		
Diététique	Gestion des menus	Lague	Restrictions		UX-09/Salle info				P	2	4	2	OUI	
Diététique	Gestion des menus	Lague	Menus	MenuPlus	UX-10/Salle info	Index/patient		NON	E	3	4	2	OUI	
Diététique	Gestion des menus	Cote globale du processus								3	4	2		

Tableau 8 : Exemple de matrice de catégorisation

4.6 Analyse et validation des résultats

L'équipe de projet organise un atelier de validation avec les gestionnaires des unités administratives visées et des archivistes afin de valider les évaluations DIC proposées. Il importe de réaliser un atelier regroupant plusieurs gestionnaires (groupe de 5 à 10 personnes) afin d'obtenir différents points de vue et de valider la catégorisation selon plusieurs perspectives. Cet atelier débute par une courte introduction expliquant la démarche, les seuils d'impact et le contenu de l'annexe 1.

Une fois la matrice de catégorisation validée, l'équipe de projet produit les résultats de la catégorisation.

L'équipe de projet transmet les résultats finaux aux gestionnaires des unités administratives visées pour une approbation préalable à l'approbation finale par le comité PRP et sécurité.

4.7 Présentation et approbation des résultats

Les résultats sont présentés au comité de PRP et de sécurité pour approbation finale. Par la suite, les résultats sont présentés à la direction générale.

Pour les établissements qui ont planifié la réalisation d'un état de la situation de leur PRP et de leur sécurité ainsi que d'une analyse de risques, ce serait le moment approprié de les faire avant de déterminer les mécanismes à appliquer. À cette fin, se référer au Guide d'élaboration du plan directeur de sécurité de l'information. En effet, l'exercice de catégorisation n'inclut pas l'évaluation de scénarios de risques spécifiques et ne tient pas compte des mécanismes déjà en place au sein de l'établissement.

De ce fait, les établissements ayant cerné des besoins de protection importants auront avantage à réaliser une analyse de risques approfondie afin de déterminer l'écart entre les mécanismes que l'établissement a déjà en place et les mécanismes qui devraient être mis en place. Cela leur permettra de cerner plus précisément leurs besoins en fonction du contexte d'utilisation, du niveau des seuils de catégorisation retenus à l'étape précédente et d'exercer ainsi une sélectivité accrue dans le choix des mécanismes de PRP et de sécurité à mettre en place en fonction de leur environnement et de leur contexte d'utilisation spécifique.

À cette étape, il s'agit pour l'établissement de sélectionner les mécanismes de PRP et de sécurité appropriés correspondant aux fonctions de sécurité requises pour protéger les documents et les systèmes d'information au niveau déterminé au cours de l'exercice de catégorisation et répondant aux exigences légales relevées précédemment.

5. Conclusion

Le Guide de catégorisation vise l'atteinte des objectifs de protection de renseignements personnels et de sécurité précisés dans le « Cadre global », « *Volet-Protection des renseignements personnels* » et « *Volet-Sécurité* » et dans la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale du SCT, datée du 23 novembre 1999. La démarche proposée s'inscrit dans les exigences de protection de renseignements personnels et dans le modèle de gestion de la sécurité des documents et actifs informationnels comme une étape préalable au choix des mécanismes à mettre en place afin de répondre aux standards gouvernementaux et ministériels en matière de protection des renseignements personnels et de sécurité. Cette démarche peut servir d'étape préparatoire à un exercice d'analyse de risques en utilisant la méthodologie proposée à l'intérieur du « Guide d'élaboration du plan directeur de sécurité de l'information-Trousse d'outils ».

La démarche proposée dans ce guide vise à faciliter le travail de catégorisation en offrant un processus basé sur les domaines d'activités de l'établissement. Particulièrement, elle suggère aux établissements :

- Une démarche visant à faciliter la réalisation des travaux requis par la catégorisation des documents et actifs informationnels ;
- Pour chacune des étapes, des encadrés qui résument les activités ;
- Un lexique (annexe 2) ;
- Une liste des lois (annexe 3) ;
- Un exemplaire du « Formulaire d'inventaire et de catégorisation » (annexe 4) ;
- Un exemplaire de la matrice de catégorisation (annexe 5).

Ce guide ne peut cependant pas couvrir tous les cas possibles et s'appliquer de manière intégrale pour tous les documents ou actifs informationnels qu'un établissement voudrait catégoriser. Il sera nécessaire que chaque établissement l'adapte en fonction de son contexte particulier.

Il offre cependant une série d'outils qui peuvent servir de barème afin de permettre à une équipe de projet de procéder à la catégorisation de l'information de son établissement et d'obtenir la base d'information nécessaire pour procéder à l'évaluation des risques et à la détermination des mécanismes qui devront être implantés.

Annexe 1 Définition des seuils d'impact

Disponibilité

Niveau 1	Niveau 2	Niveau 3	Niveau 4
<p>Il est acceptable qu'en cas de problèmes, le système d'information ne soit pas disponible pendant une période prolongée. Aucun impact sur les opérations de l'établissement.</p> <p>La panne ou l'inaccessibilité de l'information sont égales ou supérieures à 48 heures.</p>	<p>En cas de problèmes, la période de non disponibilité peut être élevée sans causer de problèmes significatifs aux opérations d'un établissement. Cependant, au-delà d'une certaine période d'indisponibilité, les opérations de l'établissement pourraient être perturbées sans toutefois nuire à sa mission.</p> <p>La panne ou l'inaccessibilité de l'information sont inférieures à 48 heures.</p>	<p>En cas de problèmes, une courte période d'indisponibilité est permise au-delà de laquelle la mission de l'établissement pourrait être sérieusement affectée. Des mesures doivent être prises pour identifier et corriger les causes du délai.</p> <p>La panne ou l'inaccessibilité de l'information sont inférieures à 4 heures.</p>	<p>Le système doit continuellement être disponible. Un effort constant doit être consenti pour s'assurer d'une disponibilité maximale.</p> <p>La panne ou l'inaccessibilité de l'information sont inférieures à 30 secondes (99.999% de disponibilité). À la limite, le système ne peut être indisponible que pour quelques minutes seulement.</p>
Exemples:			
<p>Documents à usage interne</p> <ul style="list-style-type: none"> • Notamment s'ils existent concurremment sous format papier : <ul style="list-style-type: none"> - Liste d'employés - Catalogues de centres documentaires - Formulaires, documents types • Notamment si leur disponibilité ou leur perte n'a pas de conséquences immédiates : <ul style="list-style-type: none"> - Statistiques d'utilisation d'un site Internet - Statistiques et données consolidées - Comptes rendus et contenus de présentations de séminaires internes 	<ul style="list-style-type: none"> • Procédures internes, normes et autres documents de référence administrative • Document de travail interne (analyses, études, recherches, etc.) • Procédures opérationnelles, normes • Documents relatifs aux avantages sociaux du personnel • Documents de formation • Comptes à payer et à recevoir • Grand livre 	<ul style="list-style-type: none"> • Dossiers de la clientèle • Ententes avec les fournisseurs de soins et de services • Système d'information et bases de données qui servent directement la clientèle ex. SIATH, SIURGI, DSIE. 	<ul style="list-style-type: none"> • Documents requis pour la prestation de soins urgents • Systèmes de soins nécessitant une information continue • Documents relatifs aux mesures d'urgence et autres services essentiels • Système d'une infrastructure supportant des services essentiels • Plan de continuité ou de relève d'un service essentiel

N.B. Au moment de l'évaluation du seuil d'impact en matière de disponibilité, il importe de se questionner à savoir si le groupe de documents évalués peut être requis au préalable pour une autre activité ou un autre document dont le besoin en matière de disponibilité est plus élevé.

Formules pour le calcul des % disponibilités.

La disponibilité d'une infrastructure non redondante s'exprime de la façon suivante :

Disponibilité Totale = Disponibilité A x Disponibilité B x Disponibilité C

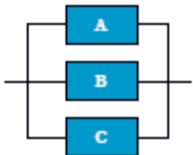


Si chacune des composantes possède une disponibilité de 99,9 %, la disponibilité totale sera de 99,7 %. Ce qui est nettement insuffisant pour supporter le niveau requis.

Lorsque les composantes sont en redondance, la disponibilité s'exprime de la façon suivante :

Disponibilité Totale = 1- ((1-Disponibilité A) x (1-Disponibilité B) x (1-Disponibilité C))

L'exemple suivant démontre la hausse substantielle de disponibilité par l'utilisation de la redondance :



Si chacune des composantes possède une disponibilité de 99,9 %, la disponibilité totale sera de 99,9999999 %. Ce qui permet de rencontrer les attentes en autant que les composantes ne soient pas du même lot. Car la probabilité de pannes dans le même intervalle de temps MTBF est élevé.

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

Le tableau suivant présente les temps de non disponibilité par année selon le % de disponibilité.

% de disponibilité	Temps de non disponibilité par année
98	7,3 jours
99	3,65 jours
99,9	8 heures. et 46 minutes
99,99	52 minutes
99,999	5 minutes et 35 secondes
99,9999	31,5 secondes

Intégrité			
Niveau 1	Niveau 2	Niveau 3	Niveau 4
La nature des informations pourrait être compromise sans que les répercussions ne dépassent les activités internes de l'administration.	La nature des informations pourrait être compromise sans que les répercussions ne dépassent les activités administratives ou d'affaires. Des mesures doivent être prises pour identifier les éventuelles pertes d'intégrité.	Des informations critiques pourraient être compromises. Il peut en découler des conséquences médicales et/ou juridiques graves. Des mesures doivent être prises pour identifier et corriger les causes de l'incident.	La nature des informations pouvant affecter la vie ou la santé d'individus est compromise. Il peut en découler des conséquences médicales et/ou juridiques graves. Un effort constant doit être consenti pour s'assurer de l'intégrité maximale de ces systèmes.
Exemples:			
<ul style="list-style-type: none"> • Informations de nature administrative sans conséquences médicales ou juridiques : - Organigrammes - Inventaires - Listes d'employés 	<ul style="list-style-type: none"> • Documents d'information de gestion, tels que : <ul style="list-style-type: none"> - Volume et types de demandes de services de la clientèle - Informations médicales et/ou financières nécessaires à la planification - Documents relatifs aux horaires de travail 	<ul style="list-style-type: none"> • Documents relatifs aux plans d'intervention • Systèmes ou documents supportant les services offerts à la population • Normes et procédures médicales et opérationnelles • Tout document ayant une valeur médicale, juridique et/ou financière 	<ul style="list-style-type: none"> • Documents contenant des informations médicales pouvant mettre en péril la santé ou la sécurité des citoyens • Documents ou systèmes contenant des informations médicales : <ul style="list-style-type: none"> - Dossiers de la clientèle - Diagnostic - Prescriptions - Groupes sanguins • Résultats de tests ou d'examens • Documents contenant des résultats d'inspection ou d'étude sur la qualité des services pouvant mettre en danger la santé ou la sécurité de personnes • Documents ayant une valeur juridique et/ou financière très importante (documents authentiques et actes officiels)

N.B. Lors de l'évaluation du seuil d'impact en matière d'intégrité, il importe de considérer la valeur juridique et le besoin d'irrévocabilité du document technologique.

En effet, la *Loi concernant le cadre juridique des technologies de l'information* prévoit que le document technologique, dont l'intégrité est assurée, a la même valeur juridique qu'un document sur support papier, dans la mesure où il respecte par ailleurs les mêmes règles de droit (par exemple, la signature des parties à un acte sous seing privé)¹².

Au moment de l'analyse du contexte, des contraintes et des exigences prévues à l'étape 2, les exigences en matière d'irrévocabilité auront normalement été établies. Il s'agit ici de vérifier plus spécifiquement le besoin d'irrévocabilité pour le groupe de documents faisant l'objet de l'évaluation. On se questionnera notamment sur les éléments suivants :

- Les documents ont-ils une valeur authentique ou un caractère officiel ?
- Les documents ont-ils une valeur médicale ?
- Les documents ont-ils une valeur financière importante ?
- Les documents engagent-ils la responsabilité de l'établissement ou de tiers avec qui il traite ?

S'il existe des besoins d'irrévocabilité et de signature, ceux-ci pourront être inscrits dans la colonne Explications/Exigences spécifiques de la partie B du Formulaire d'inventaire et de catégorisation.

¹² Article 5 de la *Loi concernant le cadre juridique des technologies de l'information*.

Confidentialité			
Niveau 1	Niveau 2	Niveau 3	Niveau 4
Les informations sont de nature publique. Aucune barrière à l'accès n'est requise.	Les informations ne sont pas assujetties à une obligation de confidentialité et/ou sont divulguées par l'établissement.	Les informations sont confidentielles en vertu d'un régime juridique. Une barrière à l'accès doit exister pour s'assurer que les accès sont contrôlés.	Les informations sont confidentielles en vertu d'un régime juridique et très sensibles à une divulgation éventuelle. Une barrière à l'accès doit exister pour s'assurer que les accès sont contrôlés et journalisés et que les informations sont cryptées.
Exemples:			
<ul style="list-style-type: none"> • Documents publics (n'étant soumis à aucune restriction d'accès prévue par la loi) • Décisions rendues publiques par l'établissement dans l'exercice de ses fonctions • Renseignements personnels à caractère public (selon l'art. 57 de la Loi sur l'accès) • Documents contenant des données statistiques sur la clientèle 	<ul style="list-style-type: none"> • Documents ayant peu d'incidences sur certaines décisions médicales ou administratives • Dans certaines circonstances, des documents contenant : <ul style="list-style-type: none"> - Un avis, une analyse - Une décision du Conseil d'administration, etc. - Détails des ententes avec d'autres établissements 	<ul style="list-style-type: none"> • Documents contenant des renseignements personnels et médicaux • Documents contenant des renseignements personnels sur la clientèle et le personnel • Rapports préliminaires d'enquête sur la clientèle et/ou sur le personnel • Certaines communications, recommandations médicales ou administratives internes, telles que recommandations portant sur la Lssss, la Loi sur l'accès • Documents de stratégie de négociation de convention collective 	<ul style="list-style-type: none"> • Documents contenant des renseignements personnels dont la divulgation causerait un tort irréparable à un individu (diagnostic du VIH, etc.) • Documents contenant des renseignements sur des enquêtes en cours, tels que : <ul style="list-style-type: none"> - Nom et coordonnées d'un informateur à la DPJ - Nom et coordonnées d'une personne bénéficiant d'un régime de protection

L'évaluation de l'impact en matière de confidentialité devrait notamment tenir compte des exigences prévues par la *Lssss* et par la *Loi sur l'accès*.

Renseignements personnels

Lorsque les documents contiennent des renseignements personnels, le seuil d'impact en matière de confidentialité doit normalement être évalué à « niveau élevé (impact grave) ».

Cependant, dans la mesure où la divulgation ou la modification non autorisée de renseignements personnels pourrait mettre en péril la sécurité ou la santé physique ou psychologique de personnes, le seuil d'impact pourrait être de niveau très élevé (extrêmement grave). On peut penser ici à la divulgation du fait qu'une personne agit à titre d'informateur pour une enquête criminelle¹³ ou aux coordonnées des personnes bénéficiant du programme de protection des témoins. On peut aussi penser à la divulgation du fait qu'une personne est atteinte du VIH ou la divulgation de certains diagnostics psychiatriques, lesquels pourraient lui occasionner un préjudice très grave.

¹³ Dans de tels cas, des textes comme la *Loi sur la protection de l'information*, L.R.C. c. O-5, pourraient trouver application.

Documents confidentiels

La Lssss prévoit que les dossiers des usagers sont confidentiels, plus généralement la *Loi sur l'accès* prévoit que certains documents doivent demeurer confidentiels alors que d'autres documents peuvent demeurer confidentiels au choix de l'établissement.

Le seuil d'impact de la confidentialité des documents qui doivent demeurer confidentiels pourrait être au minimum de niveau élevé (impact grave). Cependant, l'impact pourrait être de niveau très élevé (extrêmement grave) pour certains documents, notamment ceux dont la divulgation risque d'avoir des incidences sur l'administration de la justice ou la sécurité publique¹⁴.

Quant aux documents qui peuvent demeurer confidentiels au choix de l'établissement, l'impact pourrait être au minimum de niveau moyen (limité) et pourrait être plus élevé, selon le type de documents visés. Au moment de l'exercice de catégorisation, il ne s'agit pas nécessairement pour l'établissement de prendre une décision définitive quant au caractère confidentiel ou non de ce type de documents. Cette décision est habituellement prise dans le cadre précis d'une demande d'accès à l'information. Néanmoins, l'on pourra par prudence considérer de choisir d'appliquer un minimum de protection aux documents pouvant être confidentiels advenant que l'établissement décide subséquemment de ne pas les rendre publics.

¹⁴ Articles 28, 29 et 29.1 de la *Loi sur l'accès* ainsi que la *Loi sur la protection de l'information*.

Annexe 2 Lexique

Actif informationnel : banque d'informations électroniques, système d'information, réseau de télécommunications, technologies de l'information, installation ou ensemble de ces éléments; un équipement médical spécialisé ou ultra-spécialisé peut comporter des composantes qui font partie des documents et autres actifs informationnels, notamment lorsqu'il est relié de façon électronique à des documents et autres actifs informationnels (Réf. : *Loi sur les services de santé et les services sociaux*, art. 520.1). S'ajoutent, dans le présent cadre de gestion, les documents imprimés générés par les technologies de l'information.

Altération : toute modification qui a pour effet de changer les caractéristiques ou la nature d'une information.

Archivage de l'information : action de classer l'information dans les archives.

Audit : évaluation périodique basée sur des critères définis permettant de vérifier si les exigences de protection de renseignements personnels du Cadre global « *Volet protection des renseignements personnels* » et les normes de l'ensemble ou d'une partie du « *Volet sur la sécurité* » sont appliquées.

Authentifiant : renseignement unique à l'utilisateur et connu de lui seul, permettant d'établir la validité de l'identité d'une personne, d'un dispositif ou d'une autre entité.

Authentification : fonction de contrôle de l'accès aux documents et autres actifs informationnels permettant d'établir la validité de l'identité d'une personne, d'un dispositif ou d'une autre entité au sein d'un système d'information ou de communication.

Autorisation : attribution par une autorité de droits d'accès aux documents et autres actifs informationnels qui consiste en un privilège d'accès accordé à une personne, à un dispositif ou à une entité.

Banque d'informations électroniques : collection d'informations électroniques relatives à un domaine défini, regroupées et organisées de façon à en permettre l'accès.

Biclé : ensemble constitué d'une clé publique et d'une clé privée mathématiquement liées entre elles, formant une paire unique et indissociable pour le chiffrement et le déchiffrement des données et appartenant à une seule entité.

Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet protection des renseignements personnels : ensemble de textes encadrant la protection des renseignements personnels contenus dans des actifs informationnels et comprenant la Politique nationale sur la protection des renseignements personnels (PRP), les rôles et responsabilités des acteurs en matière de PRP ainsi que les mesures protection.

Cadre global : cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux.

Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité : ensemble de textes encadrant la sécurité des actifs informationnels et comprenant la Politique nationale sur la sécurité des actifs informationnels, les rôles et responsabilités des acteurs en matière de sécurité, les mesures en matière de sécurité des actifs informationnels et le répertoire des procédures optionnelles en cette matière.

Catégorie : classe dans laquelle on range des objets de même nature.

Catégorisation : classement par catégories. Processus d'assignation d'une valeur à certaines caractéristiques d'une information, lesquelles caractérisent le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder (définition du SCT).

Chiffrement : opération qui consiste à rendre une information inintelligible, de façon qu'elle ne puisse être lue par une personne qui ne possède pas le dispositif permettant de la ramener à sa forme initiale.

Classification : organisation intellectuelle des grandes activités d'une organisation.

Clé privée : composante de la bicyclette, laquelle composante est connue de son unique propriétaire et utilisée par lui seul pour déchiffrer un message dont il est le destinataire ou pour signer un message dont il est l'émetteur.

Clé publique : composante de la bicyclette, laquelle composante est stockée dans un répertoire accessible à tous les membres d'un réseau ou d'une organisation et permet de transmettre en toute confidentialité des messages à son unique propriétaire ou d'authentifier à l'arrivée des messages émis par ce dernier.

CNPRPS : comité national de protection des renseignements personnels et de sécurité.

Code d'identification : type d'identifiant. Groupe alphanumérique, unique et normalisé permettant d'identifier l'utilisateur d'un actif informationnel.

Collecte d'information : action de rassembler des informations variables destinées à un traitement.

Confidentialité : propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées.

Conservation de l'information : action de maintenir l'information intacte.

Copie de sécurité : copie d'un fichier ou d'un ensemble de fichiers mis à jour à intervalles réguliers en vue d'assurer la restauration des données en cas de perte.

Coupe-feu ou garde-barrière ou bastion de sécurité : dispositif informatique qui permet le passage sélectif des flux d'information entre un réseau interne et un réseau public ainsi que la neutralisation des tentatives de pénétration en provenance du réseau public.

Cryptographie : discipline qui comprend les principes, les moyens et les méthodes de transformation des données afin d'en dissimuler le contenu, d'en prévenir les modifications non détectées ou d'en éviter l'utilisation non autorisée.

Cycle de vie de l'information : période de temps couvrant toutes les étapes d'existence de l'information, soit la collecte, l'accès ou la consultation, la modification ou la rectification, la communication ou la transmission et la conservation, y inclus l'archivage ou la destruction.

Déchiffrement : action de rendre sa forme originale à une information précédemment chiffrée.

Destruction de l'information : action de faire disparaître l'information.

Détenteur : personne qui est en situation d'exercer un contrôle sur un document ou un actif informationnel.

Disponibilité : propriété qu'ont les actifs informationnels d'être atteignables et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

Document : objet constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle

est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcritibles sous forme de mots, de sons ou d'images ou en un autre système de symboles.

Document technologique : une information délimitée et structurée de façon logique sur un support faisant appel aux technologies de l'information, intelligible sous forme de mots, de sons ou d'images. Est assimilée au document technologique toute banque de données dont les éléments structurants permettent la création de documents par la délimitation ou la structuration de l'information qui y est inscrite.

Donnée : élément de base constitutif d'un renseignement, d'une information.

Donnée confidentielle : donnée qui ne peut être communiquée ou rendue accessible qu'aux personnes ou autres entités autorisées.

Donnée nominative : information relative à une personne physique identifiée ou identifiable.

Donnée publique : donnée ne faisant pas l'objet de restriction d'accès.

Donnée sensible : donnée dont la divulgation, l'altération, la perte ou la destruction risquent de paralyser ou de mettre en péril soit un service, soit l'organisation elle-même qui, de ce fait, devient vulnérable.

Droit d'auteur : droit exclusif que détient un auteur ou son représentant d'exploiter une œuvre pendant une durée déterminée.

Équipement informatique : ordinateurs, mini-ordinateurs, micro-ordinateurs, postes de travail informatisés et leurs unités ou accessoires périphériques de lecture, d'emmagasinage, de reproduction, d'impression, de communication, de réception et de traitement de l'information et tout équipement de télécommunications.

Exploitation informatique : unité administrative qui a comme tâche d'assurer le bon fonctionnement, le développement et l'entretien des services informatiques de l'établissement.

Fournisseur – prestataire – tiers : corporation, société, coopérative ou personne physique faisant affaires et étant en mesure de contracter avec le gouvernement, une unité administrative d'un établissement ou tout fonds spécial qui fournit des services ou des biens à un détenteur, à un utilisateur ou à un autre fournisseur.

Habilitation : comprend la définition d'un cadre et attribution des autorisations dans ce cadre, soit les privilèges qui sont accordés à un usager.

Identifiant : renseignement sur l'utilisateur, lequel renseignement est connu de l'établissement et permet à cet utilisateur d'avoir accès à des actifs informationnels.

Identification : fonction du contrôle de l'accès aux actifs informationnels permettant d'attribuer un code d'identification, ou identifiant, à un utilisateur, à un dispositif ou à une autre entité.

Incident : événement ayant pu mettre ou ayant mis en péril la protection des renseignements personnels et/ou la sécurité d'un ou de plusieurs documents ou actifs informationnels.

Information : élément de connaissance descriptif d'une situation ou d'un fait, résultant de la réunion de plusieurs données.

Information électronique : information sous toute forme (textuelle, symbolique, sonore ou visuelle) dont l'accès et l'utilisation ne sont possibles qu'au moyen des technologies de l'information.

Infrastructure commune : ensemble des composantes matérielles, logicielles, technologiques et organisationnelles partagées en tout ou en partie par le ministère de la Santé et des Services sociaux et les établissements du réseau de la santé et des services sociaux.

Installation : ensemble des objets, appareils, bâtiments et autres éléments installés en vue de l'utilisation d'une technologie de l'information.

Intégrité : propriété d'une information ou d'une technologie de l'information de n'être ni modifiées, ni altérées, ni détruites sans autorisation.

Interrogation de l'information : question ou ensemble des questions posées à une banque d'information.

Irrévocabilité : propriété d'un acte d'être définitif et clairement attribué à la personne qui l'a accompli ou au dispositif avec lequel il a été accompli.

Journal : relevé chronologique des opérations informatiques, constituant un historique de l'utilisation des programmes et des systèmes sur une période donnée.

Journalisation : enregistrement dans un journal de tous les accès fructueux et infructueux à un ordinateur et aux données, de l'utilisation de certains privilèges spéciaux relatifs à l'accès et des changements apportés aux actifs informationnels, en vue d'une vérification ultérieure.

Logiciel : ensemble des programmes, des procédures et des règles ainsi que de la documentation qui leur est associée, nécessaires à la mise en œuvre d'un système de traitement de l'information.

Logiciel d'application : logiciel conçu pour répondre à un ensemble de besoins dans un domaine donné.

Lssss : *Loi sur les services de santé et les services sociaux* (L.R.Q., c. S-4.2).

Matériel : ensemble des éléments physiques employés pour le traitement de l'information.

Mécanisme : agencement ou ensemble de processus et de ressources humaines, matérielles et autres disposé de façon à obtenir un résultat donné.

Mesure : disposition ayant pour but de protéger ou de conserver un actif informationnel.

Métadonnées : donnée qui renseigne sur la nature de certaines autres données et permettant ainsi leur utilisation pertinente.

Modification de l'information : action de faire des changements dans l'information.

Mot de passe : authentifiant prenant la forme d'un code alphanumérique attribué à un utilisateur, permettant à ce dernier d'obtenir l'accès à un ordinateur en ligne et d'y effectuer l'opération désirée. Cet authentifiant représente une liste secrète de caractères qui, combinée à un code d'utilisateur public, forme un identificateur unique désignant un utilisateur particulier.

Non-répudiation : voir Irrévocabilité.

Normes et pratiques : lois et règlements. Également, énoncés généraux émanant de la direction d'une organisation et indiquant ce qui doit être appliqué relativement à la PRP et à la sécurité des actifs informationnels.

Organisme : le ministère de la Santé et des Services sociaux, les Agences de développement de réseaux locaux de services de santé et de services sociaux et les établissements du réseau de la santé et des services sociaux.

Personne : une personne physique ou une personne morale de droit public ou de droit privé.

Personnel : ensemble des ressources humaines, rémunérées ou non, qui assument la mission de l'établissement.

Plan de reprise après sinistre : document qui prévoit toutes les circonstances entraînant une interruption de service des actifs informationnels ainsi que toutes les mesures applicables afin d'assurer, sur site ou hors site, les services essentiels.

Plan de sauvegarde : plan contenant les règles détaillées et strictes relatives à tous les aspects de la sauvegarde informatique (responsabilité, exhaustivité, cohérence, fichiers stratégiques, nombre de générations, cycles de rotation, confection, supports, transport, lieu d'entreposage, durée d'entreposage, accessibilité, exploitabilité, contrôles et validation).

Politique de protection des renseignements personnels : énoncé des droits et obligations des établissements et des personnes à l'égard de la protection des renseignements personnels.

Politique de sécurité : énoncé général émanant de la direction d'une organisation et indiquant la ligne de conduite adoptée relativement à la sécurité, à sa mise en œuvre et à sa gestion.

Progiciel : ensemble complet de programmes informatiques munis de documents, conçus pour être fournis à plusieurs utilisateurs et commercialisés en vue d'une même application ou d'une même fonction.

Processus : regroupement d'événements d'affaires, agencés selon une logique de création de valeur, exécutés dans le but de livrer un résultat (définition CT « architecture d'entreprise gouvernementale »).

Programme informatique : série de fonctions et de définitions en langage machine ou dans un langage plus évolué.

Registre d'autorités : contient les titres de fonctions (rôles) de l'organisation et précise les pouvoirs qui sont délégués à leur titulaire.

Renseignement : synonyme d'information.

Renseignement confidentiel : tout renseignement qui ne peut être communiqué ou rendu accessible qu'aux personnes ou autres entités autorisées.

Renseignement personnel ou nominatif : tout renseignement qui concerne une personne physique et qui permet de l'identifier.

Répertoire des procédures optionnelles : ensemble des recommandations et des suggestions relatives à la mise en place des procédures visant à assurer la sécurité des actifs informationnels.

Réseau étendu : réseau local qui devient une partie d'un réseau étendu lorsqu'une liaison est établie (par l'intermédiaire de modems, d'aiguilleurs distants, de lignes téléphoniques, de satellites ou d'autres connexions) avec un gros système, un réseau de données public ou un autre réseau local.

Réseau informatique : ensemble des composantes et des équipements informatiques reliés par voie de télécommunications, soit pour accéder à des ressources ou à des services informatisés, soit pour en partager l'accès.

Réseau local : réseau informatique de taille réduite et, le plus souvent, à l'intérieur d'un établissement ou d'un organisme.

Réseau privé : réseau appartenant à une seule organisation.

Réseau public : réseau partagé par plusieurs organisations et appartenant généralement à un fournisseur de services de télécommunications.

RSSS : réseau de la santé et des services sociaux.

RTSS : réseau de télécommunications sociosanitaire.

Sceau électronique : bloc de données dont le contenu est le résultat d'un calcul complexe effectué à partir d'un message à transmettre, qui est ajouté à ce message par l'expéditeur et dont un nouveau calcul à l'arrivée permet de vérifier l'origine et l'intégrité du message auquel il a été attaché.

Scellement : action qui consiste à adjoindre à un message à transmettre un sceau électronique permettant de garantir l'origine et l'intégrité de ce message.

Signature numérique ou signature électronique : données annexées à un document électronique qui permettent à la personne qui reçoit ce document de connaître la source des données, d'en attester l'intégrité et de s'assurer de l'adhésion de l'émetteur au

contenu de ce document. On emploie parfois l'expression signature électronique sécurisée.

Système d'information : ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

Technologie de l'information : tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

Télécommunication : ensemble des procédés électroniques de transmission d'information à distance.

Traitement de l'information ou traitement des données : ensemble des opérations effectuées automatiquement sur des données afin d'en extraire certains renseignements qualitatifs ou quantitatifs.

Transaction : opération impliquant une modification de l'information.

Transmission d'information : action de transporter une information d'un émetteur vers un récepteur.

Utilisateur : personne, groupe ou entité administrative qui fait usage d'un ou de plusieurs actifs informationnels appartenant aux établissements du réseau de la santé et des services sociaux.

Utilisation : terme qui recouvre, le cas échéant, l'ensemble des événements constituant le cycle de vie de l'information, soit la collecte, l'accès ou la consultation, la modification ou la rectification, la communication ou la transmission et la conservation, y inclus l'archivage ou la destruction.

Vérification : évaluation ciblée d'une situation problématique ou jugée à risque et ne visant que les actifs informationnels en cause.

Virus : programme inséré dans un système informatique afin de causer des dommages nuisibles et néfastes.

Annexe 3 Liste des principales lois régissant le réseau socio-sanitaire québécois ou ayant un impact sur la protection des renseignements personnels

- *Charte canadienne des droits et libertés de la personne*, [Partie 1 de la *Loi constitutionnelle de 1982* (Annexe B de la *Loi de 1982 sur le Canada* (1982, R.-U, c. 11))]
- *Charte des droits et libertés de la personne*, L.R.Q, c. C-12.
- *Code civil du Québec*, L.Q., 1991 c. 64.
- *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q. c. C-1.1.
- *Loi sur les services de santé et les services sociaux*, L.R.Q. c. S-4.2.
- *Loi sur les services de santé et les services sociaux pour les autochtones Cris*, L.R.Q. c. S-5.
- *Loi médicale*, L.R.Q. c. M-9.
- *Loi sur le protecteur des usagers en matière de santé et de services sociaux*, L.R.Q. c. P-31.1.
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q. c. A-2.1.
- *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. c. P-39.1.
- *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.
- *Loi sur les archives*, L.R.Q. c. A-21.1.
- *Loi sur les commissions d'enquêtes*, L.R.Q. c. C-37.
- *Loi sur le vérificateur général*, L.R.Q. c. V-5.01.
- *Loi sur l'équilibre budgétaire du réseau public de la santé et des services sociaux*, L.R.Q. c. E-12.0001.
- *Loi sur la santé publique*, L.R.Q. c. S-2.2.
- *Loi sur les laboratoires médicaux, la conservation des organes, des tissus, des gamètes et des embryons et la disposition des cadavres*, L.R.Q. c. L-0.2.
- *Loi sur les services préhospitaliers d'urgence*, L.R.Q. c. S-6.2.
- *Loi sur l'Institut national de la santé publique*, L.R.Q. c. I-13.1.1.
- *Loi sur la protection des personnes dont l'état mental présente un danger pour elle-même ou pour autrui*, L.R.Q. c. P-38.001.
- *Code des professions*, L.R.Q. c. C-26.
- *Loi sur la protection de la jeunesse*, L.R.Q. c. P-34.1.
- *Loi sur les jeunes contrevenants*, L.R.C. c. Y-1.
- *Loi sur le système de justice pénale pour les adolescents*, L.C. 2002, c. C.1.
- *Loi sur le curateur public*, L.R.Q. c. C-81.
- *Loi sur la Régie de l'assurance maladie du Québec*, L.R.Q. c. R-5.
- *Loi sur l'assurance maladie*, L.R.Q. c. A-29.
- *Loi sur Héma-Québec et le comité d'hémovigilance*, L.R.Q. c. H-1.1.
- *Loi sur l'assurance-médicaments*, L.R.Q. c. A-29.01.

ANNEXE 4 Exemple du
« Formulaire d'inventaire et de catégorisation »

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

<input type="checkbox"/> FORMULAIRE D'INVENTAIRE ET DE CATÉGORISATION						
Partie A : INVENTAIRE						
Nom de l'unité administrative :				Nom du détenteur :		
Nom du processus d'affaires :				Gestion centralisée/décentralisée de la sécurité logique :		
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP? <input type="checkbox"/>
						Inscrit au calendrier de conservation : <input type="checkbox"/>
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP? <input type="checkbox"/>
						Inscrit au calendrier de conservation : <input type="checkbox"/>
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP? <input type="checkbox"/>
						Inscrit au calendrier de conservation : <input type="checkbox"/>
Nom du document :	D	I	C	Papier : <input type="checkbox"/>	Électronique : <input type="checkbox"/>	Présence de PRP? <input type="checkbox"/>
						Inscrit au calendrier de conservation : <input type="checkbox"/>
Nom des systèmes d'information supportant le processus :				Nom des composantes de support		Localisation
<u>Localisation des documents physiques</u>						
Nom du document ou groupe de documents			Description des mécanismes de rangements			
<u>Alimentation d'un autre processus (système ou document)</u>				Alimentation vers un autre processus		
Nom du processus (système ou document) :				Nom du processus :		
Catégorisation du processus :	D	I	C	Moyen de transmission :		Commentaires :
Moyens de transmission :						
Partie B: CATÉGORISATION						
<i>CRITÈRES</i>	<i>CATÉGORISATION</i>				<i>EXPLICATIONS/EXIGENCES SPÉCIFIQUES</i>	
	Bas ----->Très élevé					
<i>DISPONIBILITÉ</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>		
<i>INTÉGRITÉ</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>		
<i>CONFIDENTIALITÉ</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>		

**Annexe 5 Exemple de la
« Matrice de catégorisation »**

Catégorisation des documents et autres actifs Informationnels aux fins de la protection des renseignements personnels et de la sécurité

Unité administrative	Processus d'affaires	Détenteur	Documents ou groupes de documents	Systèmes d'information	Localisation (serveurs/composantes)	Intrant	Extrant	Gestion centralisée (O ou N)	Type de document (P ou E)	Seuils d'impact			Processus sélectionné	Date de création/MAJ
										D	I	C		

