www.inforoute-gouvernementale.qc

Architecture gouvernementale de la sécurité de l'information numérique (AGSIN)

Architecture cible globale

L'inforoute gouvernement@le

Secrétariat du Conseil du trésor
Québec

Secrétariat du Conseil du trésor

ARCHITECTURE GOUVERNEMENTALE DE LA SÉCURITÉ DE L'INFORMATION NUMÉRIQUE (AGSIN)

ARCHITECTURE CIBLE GLOBALE

version 1.0

BL3_sct_v1.0p2.7.doc

DIFFUSION RESTREINTE

Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles

Québec

Septembre 2001

Table des matières

[1] Le lecteur prendra note que les normes et standards identifiés dans ce document ne le sont, dans une première étape, que pour des fins indicatives. Une étape ultérieure de validation sera nécessaire afin de statuer de façon consensuelle sur la pertinence d'adopter chacune des normes et chacun des standards identifiés, élaborer la façon de les mettre en place et identifier les impacts de leurs mises en place.

1. INTRODUCTION

Les technologies de l'information ne sont plus simplement un outil administratif supportant des opérations d'usage interne, elles sont devenues un outil stratégique. En effet, selon les technologies mises en place et selon leur arrimage avec les objectifs d'affaires, une organisation peut être propulsée en avant ou s'enliser dans les problèmes. Internet, et plus particulièrement la prestation électronique de services (PES) protégée, est en train de faire la démonstration fulgurante que les organisations deviennent tributaires des nouvelles technologies de l'information et des communications.

Le Secrétariat du Conseil du trésor (SCT) reconnaît, quant à lui, que les technologies de l'information affectent profondément les façons de faire de l'État et ont des impacts sur l'ensemble des secteurs d'activités du gouvernement. Dans son plan d'action gouvernemental, il cherche à tirer pleinement profit de cette révolution technologique dans la façon dont l'État produira et dispensera désormais ses services aux citoyens (individus) et aux entreprises. Il préconise que l'État québécois demeure un utilisateur modèle et transige de façon électronique avec les individus et entreprises. De plus, il souhaite créer un climat de confiance envers ce nouveau mode d'affaires.

Afin de concrétiser cette vision axée sur les individus et les entreprises, le SCT a entrepris en collaboration avec les ministères et organismes (M/O), un exercice d'architecture à haut niveau nommé architecture d'entreprise gouvernementale (AEG) qui, en fonction des grands objectifs gouvernementaux, vise à comprendre et illustrer quelle sera la nouvelle prestation de services et ses impacts sur les grands processus et les ressources informationnelles. L'architecture d'entreprise gouvernementale comporte plusieurs volets et segments dont l'un consiste en une architecture gouvernementale de la sécurité de l'information numérique (AGSIN) visant d'une part à assurer la sécurité des renseignements personnels et la confiance des individus à l'égard de la protection de ces renseignements et de la vie privée et, d'autre part, à supporter la mise en place des grandes orientations gouvernementales.

Outre l'AGSIN, plusieurs initiatives gouvernementales ont été entreprises au Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles (SSIGRI) du SCT afin d'appuyer les ministères et organismes dans leur mandat de mise en œuvre de la sécurité. Les efforts ont porté presque essentiellement sur la mise en œuvre de la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale*, telle qu'adoptée par le Conseil du trésor le 23 novembre 1999 en remplacement de l'ancienne directive de 1993.

Le plan d'action gouvernemental en cours de réalisation porte sur deux axes d'intervention soit ceux de la gouverne et de soutien aux M/O.

En ce qui concerne l'axe de gouverne, les travaux ont porté principalement sur :

- La mise en place d'un comité gouvernemental sur la sécurité et, notamment, sur l'établissement des objectifs de ce comité, sa composition et son mode de fonctionnement.
- Un modèle sur l'organisation et la gestion de la sécurité qui présente la définition des besoins de sécurité dans les M/O dont l'analyse de risques, l'état de la sécurité existante, le plan global de sécurité et enfin le bilan de sécurité. Ce modèle traite également des services que le Secrétariat doit rendre aux M/O en matière de sécurité de l'information.
- Un guide pour la préparation du bilan annuel en sécurité qui fera état des principaux éléments de suivi, dont entre autres la qualité des mesures en place, les coûts de la sécurité, les incidents de sécurité vécus et les progrès réalisés.

- La préparation d'un formulaire pour réaliser une enquête auprès des M/O afin de valider leurs priorités d'action en sécurité de l'information numérique et des échanges électroniques notamment quant à un programme de formation, à des outils de sensibilisation et à d'autres guides nécessaires à la réalisation de leur mandat en sécurité.
- La collaboration dans la préparation du cahier des charges dans le cadre du projet d'architecture de sécurité des échanges électroniques (AGSIN).

En ce qui concerne l'axe de soutien, plusieurs travaux ont été réalisés pour développer des outils d'aide permettant aux M/O de mieux comprendre et réaliser leurs mandats découlant des responsabilités énoncées dans la Directive. À cet effet, les travaux suivants ont été mis en priorité et réalisés en collaboration avec les M/O :

- La tenue entre décembre 2000 et juin 2001 de quatre réunions d'information et de sensibilisation pour les responsables de la sécurité de l'information numérique (RSIN) et les responsables de la mise en œuvre de la Directive (RMOD).
- La tenue en mars et avril 2001 de 15 séances de formation pour les RSIN et les RMOD.
- La préparation d'un modèle et la précision des considérations pour la définition d'un réseau de partage et de vigie en sécurité et une proposition d'un plan de mise en œuvre.
- La préparation du *guide sur la catégorisation de l'information et des mesures généralement appliquées en sécurité* afin d'aider les M/O à mettre en place rapidement des mécanismes pour assurer un minimum de sécurité.
- L'analyse des méthodes et des outils d'identification et de gestion des risques afin d'appuyer les recommandations d'approche de gestion des risques du SCT auprès des M/O.
- Une étude sur la *Sécurité & Certification de conformité des sites WEB* afin d'identifier les raisons pour lesquelles il est opportun de recourir à la certification des sites Web, d'identifier les principaux acteurs oeuvrant dans le domaine de la certification des sites Web, d'expliciter les finalités de leurs activités de certification, d'identifier les principes et critères de certification, d'exposer les méthodes, la portée et les effets de la certification et finalement d'identifier les risques et les limites de la certification des sites Web .
- Une grille d'évaluation de la sécurité des sites Web qui vise à sensibiliser, à informer et à guider les webmestres dans l'évaluation de la sécurité des infrastructures des sites Web gouvernementaux dont ils sont responsables.
- Le développement des compétences des ressources humaines en sécurité et plus précisément sur la définition du profil de compétence d'un responsable de la sécurité de l'information numérique et des échanges électroniques.
- L'accompagnement auprès des M/O pour des avis sur leurs projets traitant de sécurité.

1.1 Mise en contexte

1.1.1 Contexte

Comme le gouvernement a choisi de favoriser l'utilisation des inforoutes pour offrir de meilleurs services aux individus et aux entreprises, il est primordial de revoir les façons de faire de l'État. Le virage vers la modernisation de l'appareil gouvernemental est déjà amorcé et constitue certainement le facteur le plus

déterminant dans l'élaboration d'une architecture d'entreprise gouvernementale. Le développement harmonieux de ce plan gouvernemental, en considérant les contraintes budgétaires, nécessite la mise en œuvre d'un cadre intégrateur.

En voici les principales caractéristiques:

- La vision de l'État réseau: l'État réseau est un concept virtuel visant à fournir aux différents M/O une direction stratégique dans le but de dispenser dans le futur des services de nature à faciliter la vie des individus et des entreprises. L'exemple le plus simple est l'unification d'un service de changement d'adresse qui informerait tous les M/O concernés par l'intermédiaire de mécanismes transparents pour l'individu. Dans ce contexte, l'État réseau nécessite des transformations profondes dans les processus de travail, les applications et les infrastructures.
- La concrétisation de l'État réseau: la transformation profonde des façons de faire de l'État doit s'accompagner d'une identification et d'une prise en charge des impacts de cette transformation sur les ressources humaines et sur les autres aspects de l'organisation. Ainsi, le passage d'une pratique de multiservices en un seul service, de procédures fermées à une interrelation organisationnelle, de données séparées en des données partagées, d'un traitement local en un traitement «interconnecté» sont autant de façons d'aborder le dossier dans le but évident de concrétiser la vision de l'État réseau.
- Le focus sur les composantes communes, partageables et réutilisables: il existe un foisonnement de projets d'investissement porteurs qui sont en cours d'élaboration ou de réalisation à l'échelle gouvernementale. Il faut pouvoir identifier leur potentiel de mise en commun, de partage et de réutilisation et planifier les actions pour les insérer activement au chapitre des initiatives à encourager et à soutenir comme moteurs des changements.
- La force de l'échange électronique: L'évolution rapide des technologies de l'information et des télécommunications permet aux ministères et organismes d'envisager des changements dans le traitement de l'information, comme la carte à microprocesseur d'accès au dossier, le dossier citoyen informatisé, différents dépôts de données, l'intégration des données en fonction de résultats, le télétraitement, l'inforoute de la géomatique, etc. L'utilisation de ces diverses technologies va faciliter le développement de liens plus étroits, plus intégrés, entre les M/O tant sur le plan de leur mission que sur le plan administratif, et ce tant sur le plan local que régional ou national. Enfin, elles permettront de mieux évaluer la pertinence, l'efficacité et l'efficience des services aux individus et entreprises.
- La maîtrise des coûts: bien que l'évolution des dépenses soit contrôlée depuis quelques années, la maîtrise des coûts demeure une variable importante. Le gouvernement québécois veut atteindre le déficit zéro et, comme les dépenses de fonctionnement du gouvernement représentent une part significative des dépenses de programmes, la maîtrise de ces dépenses est prioritaire.
- L'angle du service aux individus et aux entreprises: les ministères et organismes, comme toutes les grandes organisations, changent leurs façons d'offrir les services. On se dirige vers la création de réseaux intégrés de services, le développement d'approche-programme et la décentralisation des services, etc. L'intention de faciliter les communications et les transactions électroniques entre l'État, les individus et les entreprises s'accompagne de mesures prises dans le but de simplifier et rendre plus transparent l'accès aux informations et services du gouvernement.
- La sécurité et la protection de l'information: L'État est amené à colliger des renseignements personnels et confidentiels sur les individus et les entreprises pour l'administration de ses nombreux programmes. Ces particularités posent de grands défis à l'État dans le déploiement technologique. Le développement de la confiance envers les échanges électroniques gouvernementaux est primordial.

Dans cette vision de l'État réseau, le cadre intégrateur de la démarche de l'architecture d'entreprise gouvernementale doit s'assurer que les principes de sécurité et de protection des renseignements

personnels sont impérativement préservés. En effet, la structuration et la gestion de l'information numérique doivent être réalisées en toute sécurité dans le respect des lois et règlements tout en assurant le plus de services possibles aux individus et aux entreprises (ex.: respect de la Loi d'accès à l'information).

Le projet qui a conduit à la production de ce présent document s'inscrit dans la continuité des travaux de l'architecture d'entreprise gouvernementale (AEG) et vient préciser le segment sécurité de celle-ci, en élaborant l'AGSIN.

1.1.2 Objectifs

Les principaux objectifs du projet d'AGSIN sont d'identifier et d'analyser les éléments architecturaux de haut niveau permettant au SCT de promouvoir auprès des M/O une vision commune de la sécurité de l'information numérique. Il lui permettra également de positionner sa démarche de mise en œuvre de composantes communes, partagées ou réutilisables de sécurité.

Cette vision commune doit favoriser la cohérence et la confiance pour la clientèle du gouvernement dans la prestation électronique de services, l'interopérabilité entre les organisations gouvernementales et une protection adéquate des informations numériques.

Le projet d'AGSIN propose de fournir à l'ensemble des intervenants du gouvernement du Québec oeuvrant au niveau de la sécurité une vue commune de la sécurité de l'information numérique afin de:

- Fournir une vision commune des principales composantes de la sécurité, arrimée étroitement à l'AEG et aux orientations gouvernementales en sécurité et en protection des renseignements personnels;
- Arrimer cette vision aux grandes orientations stratégiques gouvernementales;
- Alimenter un plan d'action souple en vue d'une mise en œuvre harmonieuse de l'architecture gouvernementale cible de la sécurité.

Il faudra assurer la pérennité de l'AGSIN. Le cadre méthodologique de l'AEG devra être adapté pour l'AGSIN s'il y a lieu dans ses mécanismes de suivi et d'ajustement de l'architecture, incluant une vigie constante, afin qu'elle tienne compte de l'évolution continue des façons de faire du gouvernement et de son environnement juridique, humain, organisationnel et technologique.

Plus spécifiquement ce projet consiste à :

- Présenter le contexte global de la sécurité de l'information numérique dans l'industrie et dans les gouvernements ainsi que tracer un portrait des éléments de sécurité en place ou en développement au gouvernement et des besoins de sécurité des ministères et organismes;
- Établir les orientations et les principes sur lesquels sera basée l'AGSIN au gouvernement avec ceux établis par l'AEG et les enrichir;
- Modéliser les fonctions de sécurité de l'échange de l'information numérique avec la clientèle, dont la PES, en représentant ses principales composantes et en faisant ressortir les fonctions de sécurité ainsi que les mécanismes de sécurité et solutions technologiques qui présentent un potentiel de mise en commun, de partage ou de réutilisation au niveau gouvernemental et de cohérence pour la clientèle;
- Évaluer la concordance des modèles spécifiques de l'ICPG, de GIRES et du répertoire gouvernemental en cours de développement en fonction de l'AGSIN;

- Identifier des zones de normalisation et des normes ouvertes, de facto ou émergentes pertinentes à l'AGSIN;
- Faire des recommandations sur la mise en œuvre et les suites à donner.

1.1.3 Portée

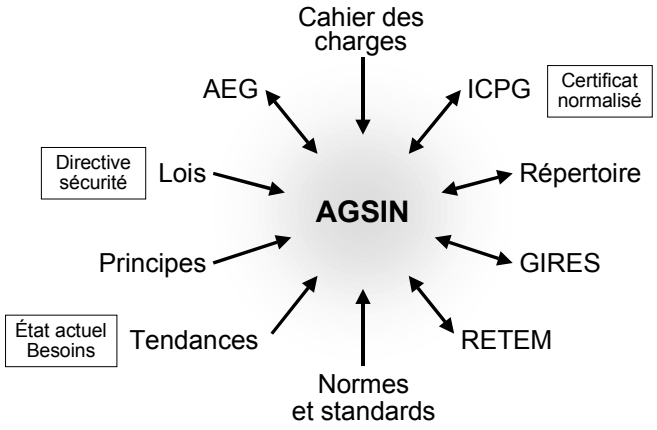
L'AGSIN se veut une architecture de haut niveau essentielle à la cohérence de l'État en matière de sécurité. Il est de la responsabilité de chaque M/O ou d'une organisation responsable d'un service d'élaborer sa propre architecture de sécurité de l'information numérique (ASIN) spécifique à son organisation.

Au moment d'effectuer ce projet, certains paramètres nécessaires à un arrimage complet des travaux avec l'AEG n'étaient pas encore définis ou étaient en cours de définition. Afin de s'assurer que les intrants nécessaires à ce projet sont adressés adéquatement, l'équipe de réalisation a retenu certaines hypothèses pour la réalisation de ce dossier, lesquelles sont:

- l'AGSIN n'a pas le mandat de préciser l'architecture d'information et d'application de l'AEG. Compte-tenu que ces travaux sont en cours d'élaboration, il sera nécessaire d'effectuer des ajustements à l'AEG et à l'AGSIN ultérieurement;
- la notion de domaine de confiance va au-delà du segment de la sécurité de l'AEG. En effet, plusieurs autres éléments doivent être pris en compte dans les relations d'affaires entre les organisations pour établir et maintenir un climat de confiance. L'AGSIN se limite à ne définir que les concepts inhérents à la sécurité;
- l'identification des composantes de nature communes, partageables et réutilisables pourra se limiter à l'énoncé de potentiels, lorsqu'il apparaît que le gouvernement devra, préalablement à la mise en œuvre:
  - procéder à certaines analyses de faisabilité technique et/ou à la normalisation d'objets particuliers;
  - procéder à l'analyse coût-bénéfice inhérent à l'usage d'une composante;
  - se prononcer quant à l'obligation de faire usage des composantes identifiées comme essentielles.

La figure suivante illustre en synthèse les principaux intrants à l'AGSIN.

INTRANTS À L'AGSIN



À leur tour, les résultats de ces travaux serviront d'intrants à une stratégie de mise en œuvre et un plan global d'amélioration de la sécurité de l'information et de protection des renseignements personnels au gouvernement.

1.1.4 Démarche

L'approche de développement de l'AGSIN prend en compte une vision globale de la sécurité, axée sur un encadrement juridique, humain, organisationnel et technologique favorisant au maximum les échanges électroniques sécuritaires des différents secteurs d'affaires. En effet, l'architecture de sécurité est analysée sous l'angle de l'information et tient compte de la nécessité d'identification/authentification et d'habilitation/contrôle d'accès des diverses parties pour la protection des renseignements personnels.

Une démarche de réalisation basée sur un partenariat étroit entre le SCT, les M/O et les experts de l'industrie a été mise de l'avant afin de faciliter l'élaboration et la promotion de l'AGSIN. Cette démarche est adaptée:

- aux exigences d'un environnement juridique, humain, organisationnel et technologique évoluant continuellement;
- à la nécessité d'identifier rapidement les enjeux stratégiques de la sécurité auxquels devront faire face le SCT et les M/O, compte tenu de ce qui se passe dans leurs organisations;
- à la nécessité d'impliquer activement les personnes clés du SCT et des M/O qui auront à prendre ces décisions stratégiques, à les appliquer et à en être imputables.

De ce fait, il est essentiel de maximiser la récupération des acquis organisationnels tout en capitalisant sur les nouvelles opportunités d'échanges et d'affaires électroniques protégés dans un monde d'informations numériques.

Ainsi, la prestation électronique de services (PES) protégée devient le fer de lance de l'architecture d'entreprise gouvernementale. À cette fin, l'AGSIN doit privilégier une architecture ouverte et flexible afin de favoriser les échanges électroniques protégés tout en respectant la protection de la vie privée par des mécanismes de sécurité appropriés.

Dans un dossier aussi complexe et nécessaire que l'architecture d'entreprise gouvernementale, une AGSIN doit prendre en considération les différentes interactions qui existent entre les clientèles et les M/O ainsi qu'entre les M/O pour les échanges électroniques protégés.

C'est ici que la vision de la sécurité d'entreprise prend tout son sens. En effet, la sécurité doit être perçue comme un moyen de faciliter l'accès sécuritaire à l'information numérique et de permettre des échanges électroniques sécurisés en toute confiance.

Ainsi, le projet d'AGSIN se compose des sept livrables suivants :

1. Portrait et besoins gouvernementaux ;
2. Orientations et principes ;
3. Architecture cible globale (le présent document) ;

4. Concordance avec l'infrastructure à clés publiques gouvernementale (ICPG) ;
5. Concordance avec le répertoire gouvernemental ;
6. Concordance avec GIRES ;
7. Recommandations de mise en œuvre.

Le présent document, architecture cible globale, se veut donc le principal et la synthèse de cette série. Il présente à cet effet :

- Un sommaire (document séparé) ;
- La définition des principaux termes utilisés dans ce document (en annexe) ;
- Un rappel des principales tendances de l'industrie en ce qui a trait à la sécurisation des infrastructures technologiques, applications et informations numériques de même que certaines tendances gouvernementales hors Québec ;
- Un rappel du contexte, portrait global et besoins en matière de sécurité de l'information numérique au gouvernement du Québec en présentant un état actuel de la situation en matière de sécurité dans les chantiers centraux, les ministères et organismes consultés et les infrastructures centrales. Il présente aussi leurs besoins de sécurité selon la dimension juridique (cadre légal), organisationnelle[2] (cadre de gestion de la sécurité) et technologique (composantes physiques et solutions technologiques) ;
- Le cadre global de référence de la sécurité ;
- Le modèle conceptuel à haut niveau de l'AGSIN ;
- L'ensemble des vues spécifiques (affaires, informations, applications et infrastructures) ;
- L'identification des potentiels de partage des composantes de sécurité (communes, partageables ou réutilisables).
- La synthèse des arrimages avec les dossiers spécifiques (ICPG, GIRES, répertoire gouvernemental et RETEM) ;

Pour mener à bien la rédaction de ce bien livrable, la démarche de réalisation s'est appuyée sur un processus de consultation, tenant compte de :

- La documentation gouvernementale pertinente au projet ;
- Les meilleures pratiques dans les autres gouvernements et dans l'industrie (Gartner, Giga, etc.) ;
- Les résultats d'ateliers de consultation, appuyés par un processus de cueillette d'information auprès des ministères et organismes représentatifs de l'administration publique[3] ;
- L'expertise de responsables d'initiatives et de projets structurants en matière de technologies dans l'administration publique.

[2] En raison de l'importance de la dimension humaine, les aspects de cette dernière seront extraits de la dimension organisationnelle et feront l'objet d'une nouvelle dimension dans la section 2 (et suivantes) du présent document.
[3] La liste des participants aux ateliers de consultation est présentée à l'annexe E.

1.2 Perspectives contextuelles

Cette section, qui constitue un rappel du document *Architecture gouvernementale de la sécurité de l'information numérique – Portrait et besoins gouvernementaux,* présente les principales tendances de l'industrie en ce qui a trait à la sécurisation de l'information numérique de même que certaines tendances gouvernementales hors Québec[4]. De plus, elle décrit le contexte gouvernemental québécois, de même que l'état actuel de la situation en matière de sécurité dans les ministères et organismes consultés, les chantiers centraux et les infrastructures centrales[5].

Notons que la pratique veut qu'on subdivise les éléments à considérer dans la sécurisation des infrastructures technologiques, des applications et des informations numériques en différents aspects de la sécurité. Le modèle holistique qui a servi de base aux perspectives contextuelles compte huit aspects (appelés domaines dans le document « Portrait et besoins gouvernementaux ») regroupés en trois dimensions distinctes soit les dimensions juridique, organisationnelle (couvrant certains aspects humains) et technologique. La section 2.4 décrit plus en détails ces dimensions, de même que les différents aspects de la sécurité qu'elles renferment. Notons qu'une quatrième dimension, la dimension humaine, a été ajoutée dans la section 2.4 afin de mettre en évidence l'importance de cette dimension dans la gestion de la sécurité[6].

1.2.1 Tendances de l'industrie

Cette section décrit les tendances de l'industrie en ce qui a trait à la sécurisation de l'information numérique. Plus spécifiquement, elle décrit un certain nombre de tendances à haut niveau et d'initiatives juridiques, organisationnelles et technologiques ayant été entreprises depuis quelques années dans l'industrie. Notons que les tendances technologiques plus spécifiques sont décrites à la section 2.5 de ce document.

1.2.1.1 Dimension juridique

Depuis quelques années, la communauté d'affaires juridiques internationale tente de résoudre un nombre important de problématiques liées au commerce électronique et à la sécurisation des informations et échanges numériques. Certaines initiatives se sont montrées particulièrement déterminantes pour l'avancement du commerce électronique et de la PES en faisant en sorte que les transactions et les informations échangées électroniquement ne fassent pas l'objet de discrimination. Les paragraphes qui suivent décrivent quelques-unes de ces initiatives.

International

Datant de 1996, la loi type sur le commerce électronique de la Commission des Nations Unies pour le droit commercial international (CNUDCI) a probablement été l'initiative la plus influente au niveau international. Plus d'une douzaine de pays et états ont mis en place une juridiction basée sur cette loi type.

[4] Les termes «en date du », «actuellement », «sont en cours », «sont envisagés», «jusqu'à ce jour », «sont réalisés » utilisés dans ce document présentent des informations en date de mai 2001.

[5] Le lecteur qui voudra obtenir plus de détails sur ces différents points devra consulter le document *AGSIN – Portrait et besoins gouvernementaux* produit dans le cadre de ce présent projet.

[6] Cet ajout a été fait suite à une recommandation du Comité gouvernemental d'orientation stratégique sur la sécurité (COSS).

De plus, le développement des lois uniformisées du Canada et des États-Unis, de même que de la directive sur un cadre communautaire pour les signatures électroniques de l'Union Européenne ont aussi été influencés par cette loi type. Notons que le gouvernement du Québec a participé aux travaux de la Commission. La Commission des Nations Unies pour le droit commercial international a aussi entrepris en 1997 des travaux pour le développement d'une loi type portant spécifiquement sur la signature électronique. Cette loi type a été approuvée en juillet 2001.

États-Unis

Approuvé en 1999 par le National Conference of Commissioners on Uniform State Laws, le Uniform Electronic Transactions Act (UETA) a été conçu afin d'éliminer tout doute concernant la force exécutoire des transactions électroniques, qu'elles soient sous la forme d'échanges commerciaux sur Internet, de transactions de crédit électronique, d'échanges électroniques de données ou de courrier électronique. L'UETA a été adoptée par plus de 23 états américains en 1999 et 2000, et une douzaine d'états supplémentaires devraient y adhérer en 2001.

Le gouvernement américain a suivi plusieurs de ses états en adoptant en juin 2000 une loi qui s'applique autant au secteur public qu'au secteur privé, le Electronic Signatures in Global and National Commerce Act. Tout comme l'UETA et les autres lois sur la signature électronique ou le commerce électronique, le E-Sign Act proscrit la discrimination contre les enregistrements et la signature électronique. Le gouvernement fédéral a aussi sur la table à dessin deux projets qui visent à favoriser les affaires électroniques, le Electronic Commerce Enhancement Act of 2001 et le Electronic Commerce Technology Promotion Act.

Union Européenne

En décembre 1999, le parlement européen a adopté la directive sur un cadre commun pour les signatures électroniques. La directive de l'union européenne exige que les lois locales des états membres se conforment d'ici juin 2001 aux principes présentés dans la directive. Elle incorpore l'approche globale et technologiquement neutre de la loi type sur le commerce électronique de l'ONU, mais touche aussi de façon spécifique les technologies de signatures sécurisées telles que la signature numérique. Parmi les législations européennes locales se conformant en partie à la directive, notons le Electronic Communications Act de l'Angleterre, la loi portant sur l'adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique de France et le Electronic Signatures in Internet Transactions Initiative d'Allemagne, qui sera effective au moment de l'adoption du nouveau code civil de l'Allemagne en juin ou juillet 2001.

Canada et provinces (autres que le Québec)

Le gouvernement fédéral propose, depuis octobre 1999, la *loi sur la protection des renseignements personnels et les documents électroniques (C-6)*[7] dans le but de supporter et promouvoir le commerce électronique. Plus précisément, elle vise la protection des informations personnelles recueillies, utilisées ou dévoilées et l'utilisation des moyens électroniques pour communiquer ou enregistrer des informations ou transactions. Une initiative parallèle à la loi C-6 est proposée par la Conférence pour l'harmonisation des lois au Canada, le projet de loi uniforme sur le commerce électronique. La Conférence a pour but de

[7] La loi C-6, qui aura certains impacts au Québec, est décrite plus en détails à la section 2.4.1.1

faire adopter la loi uniforme dans les différentes provinces. Bien qu'elle est en grande partie basée sur une loi type ayant fait ses preuves (la loi type de l'ONU), il semble que la loi uniforme se soit fait supplanter par différentes lois provinciales, de même que par la loi C-6.

Les initiatives provinciales et territoriales en matière de lois sur le commerce électronique et les documents et transactions numériques sont nombreuses. En effet, outre le Québec, la Colombie Britannique, le Manitoba, la Nouvelle-Écosse, l'Ontario, la Saskatchewan, l'Alberta, l'Île du Prince-Édouard et le Yukon proposent une loi ou un projet de loi couvrant ces thèmes.

Autres pays

Plusieurs autres pays ont adopté des lois touchant le commerce électronique ou sont en voie de le faire, particulièrement en Océanie et en Asie et, dans une moindre mesure, en Amérique du Sud.

1.2.1.2 Dimension organisationnelle

Il est fréquent lors de la réalisation d'une architecture de sécurité de ne considérer que la dimension technologique. Bien que celle-ci soit essentielle, elle ne saurait être suffisante pour assurer la sécurité des informations, des applications et des infrastructures technologiques.

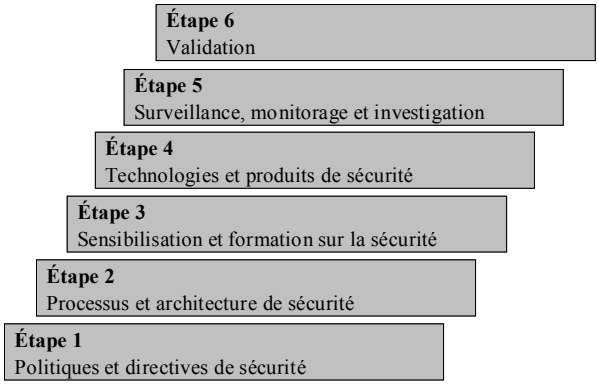
La dimension organisationnelle, certainement aussi importante que la dimension technologique, permet de contrôler, de structurer, d'orienter et de gérer la sécurité. Les normes et standards généraux de sécurité de l'industrie telles que les normes ISO/IEC 13335, ISO/IEC 7498-2 et ISO/IEC 17799[8], le « Manuel canadien de la sécurité des technologies de l'information » du centre de la sécurité des télécommunications (CST), la « norme de sécurité technique dans le domaine de la technologie de l'information » de la Gendarmerie Royale du Canada et les « Generally Accepted System Security Principles » de la International Information Security Foundation (I^2SF), tiennent compte de cette réalité. Une recherche[9] de Gartner indique que les organisations à la fine pointe de la sécurité identifient, sans exception, les politiques et standards[10] de sécurité comme les éléments fondamentaux qui doivent orienter toutes les autres activités de sécurité. Ces éléments organisationnels doivent être définis indépendamment des technologies.

La dimension organisationnelle permet non seulement de structurer et d'orienter la sécurité, mais aussi de mesurer l'efficacité des processus, des moyens et des solutions technologiques mises en place. Pour mesurer cette efficacité, il est avant toute chose indispensable, selon Gartner, qu'une organisation définisse trois éléments clés : ses buts en terme de sécurité (politique), ses standards et son canevas (architecture). Sans ces éléments, une organisation ne peut répondre facilement et de façon objective et sensée à des questions telles que « L'organisation doit-elle répondre à un incident en déployant des solutions technologiques ? », « Comment l'organisation sait-elle si elle a atteint un niveau satisfaisant de contrôle ? » « Quels efforts l'organisation est-elle prête à mettre pour réduire les risques ? » « Qui est responsable de la surveillance des applications ? », etc.

[8] On consultera l'annexe D pour plus de détails sur cette norme et tout autre norme mentionnée dans ce document.
[9] On se référera à l'article *Do Security Products Alone Solve the Problem?* de Gartner, pour plus de détails.
[10] Gartner désigne par standards une définition spécifique des besoins qui identifie des exigences telles que la définition des rôles et responsabilités, des éléments de contrôle de la sécurité de base, de la méthodologie d'évaluation des vulnérabilités (menaces/risques), de la stratégie d'escalade des incidents et du processus de déviation.

Gartner suggère de suivre les étapes décrites dans la figure suivante pour la mise en œuvre des projets de sécurité. Selon cette dernière, les organisations qui ont amorcé leurs projets sans élaborer de politiques et standards devraient immédiatement revenir sur leurs pas.

MISE EN ŒUVRE DES PROJETS DE SÉCURITÉ



Source : Gartner Group

Un cadre de gestion de la sécurité est donc essentiel à la sécurisation des infrastructures technologiques, des applications et des informations numériques. On ne peut considérer la conception d'une architecture de sécurité sans cet élément.

Finalement, la dimension organisationnelle ne saurait être complète sans considérer un certain nombre d'aspects humains tels que l'éthique, la morale, la prévention, la formation, les comportements de la clientèle, les pratiques professionnelles, l'imputabilité de l'employé, l'implication des partenaires syndicaux dans la protection de l'employé contre son environnement, ses collègues, etc. La dimension humaine est abordée plus en détails à la section 2.4.2.

1.2.1.3 Dimension technologique

Une architecture de sécurité doit englober un certain nombre de composantes physiques et de solutions technologiques ayant pour but d'assurer la sécurité des informations et des échanges numériques de même que des équipements et infrastructures d'échange et de traitement de l'information numérique. Ces logiciels, équipements et moyens de communication peuvent se décomposer en différentes classes de composantes. Ces classes sont généralement appelées services ou fonctions de sécurité dans l'industrie. Plusieurs découpages ont été proposés dans le cadre des différentes initiatives d'architectures d'entreprise et de sécurité menées mondialement. Notons par exemple :

PRINCIPALES INITIATIVES ARCHITECTURALES

Initiative architecturale	Année de publication	Découpage
North Carolina Technical Architecture	Certains chapitres en 1997 (révision en 2000) et d'autres en 2000	Identification, authentification, autorisation/contrôle d'accès, administration, audit

Initiative architecturale	Année de publication	Découpage
Ohio Enterprise Architecture	Certains chapitres en 1998, d'autres en 1999 et 2000	Identification, authentification, autorisation/contrôle d'accès, administration, audit
Architecture technique de l'information de la GRC	1999	Identification/authentification, autorisation, confidentialité, non-répudiation, intégrité des données, contrôlabilité, protection antivirus
Norme ISO/IEC 10181 - Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres de sécurité pour les systèmes ouverts[11]	1996 (partie 1 à 3 et 5 à 7) et 1997 (partie 4)	Authentification, contrôle d'accès, non-répudiation, confidentialité, intégrité, audit de sécurité et alarmes

Le découpage proposé dans cette architecture et présenté à la section 2.5 s'inspire de ces différentes initiatives.

1.2.1.4 Besoins émergents

Selon le groupe GIGA[12], la multitude des téléphones cellulaires supportant le standard Wireless Access Protocol (WAP) et la venue des réseaux à haute vitesse pour la technologie sans fil conduiront les utilisateurs de ces appareils à les utiliser davantage pour les applications Web. Les téléphones cellulaires avec des écrans couleurs plus grands et une meilleure résolution sont également des facteurs qui contribueront à une plus grande utilisation.

Cependant, il reste encore certaines considérations de sécurité relatives à l'utilisation des téléphones cellulaires pour la PES protégée. Le protocole Wireless Transport Layer Security (WTLS) est une partie du standard de l'industrie sans fil, WAP. WTLS est un proche parent du standard SSL/TLS. Il fournit les mêmes fonctionnalités de base que SSL/TLS, mais seulement du téléphone cellulaire à la passerelle WAP/Internet. Actuellement, la sécurité de bout en bout pour une transaction électronique n'est pas garantie. En effet WTLS ne gère pas l'authentification du client. Ce problème sera résolu à partir de la version 1.2 du protocole WAP et lorsque les téléphones cellulaires supporteront cette version.

Toujours au niveau de la technologie sans fil, les assistants numériques personnels et autres nouvelles technologies de ce type deviendront également des appareils intéressants pour la PES. Une veille technologique permettra de suivre l'évolution de ces appareils prometteurs.

1.2.2 Tendances gouvernementales (hors Québec)

Selon la firme NUA Internet Surveys, près de 410 millions d'individus dans le monde, soit 6,7% de la population mondiale, avait accès au réseau Internet en novembre 2000. Ces individus sont de plus en plus nombreux et habitués à utiliser Internet pour faire de la cueillette d'information et même réaliser des

[11] On consultera l'annexe D pour plus de détails sur cette norme.
[12] *Key Trends for 2001: Mobile Devices*, Giga Information Group, IdeaByte, 29 novembre 2000

transactions en ligne. Les individus et les entreprises s'attendent donc à ce que les gouvernements emboîtent le pas aux entreprises privées et utilisent eux aussi l'Internet pour délivrer leurs services.

En réponse à cette demande pressante des individus et des entreprises, les différents paliers de gouvernements, autant en Amérique et en Europe qu'en Asie ou en Océanie, ont démarré de nombreuses initiatives visant à orienter, structurer et supporter la prestation de services via différents canaux de communication (Internet, sans fil, téléphone). Dans un premier temps, plusieurs pays tels que le Canada, les États-Unis, la France, l'Angleterre, l'Australie et Singapour, ont adopté des plans de transformation de l'état où les technologies, en particulier celles liées à Internet, jouent un rôle central. De façon générale, ces plans de transformation de l'état visent à promouvoir le concept du « e-gouvernement » (gouvernement qui fournit des services électroniques aux individus, aux entreprises, à ses partenaires d'affaires et ses employés) et à indiquer les intentions des gouvernements en ce sens. Ces plans de transformation de l'état sont à la base de multiples projets de prestation électronique de services qui ont été entrepris dans ces pays. Le tableau qui suit décrit brièvement quelques-unes de ces initiatives :

PLANS DE TRANSFORMATION DE L'ÉTAT

Pays, province ou état	Plan de transformation	Exemples de PES
Angleterre	Modernising Government White Paper, e-Government Strategy	➢ National Grid for Learning : Contenu de formation et accès aux écoles et collèges. ➢ NHS Direct : Intégration d'une « ligne téléphonique santé » disponible en tout temps et d'un portail de la santé.
Australie	Governement Online - The Commonwealth Government's Strategy	➢ Paiement de factures et contraventions. ➢ Votation en ligne.
Canada	Orientations stratégiques de la gestion de l'information et de la technologie de l'information – Pour servir la population canadienne du XXIe siècle	➢ Agence des douanes et du revenue du Canada : Projet de transmission électronique des déclarations de revenu des particuliers. ➢ Poste Canada : Projet de bureau de poste électronique. ➢ Industrie Canada : Enchères du spectre de radiofréquences sur Internet
Colombie Britannique	Infosmart	➢ Guichet unique d'enregistrement d'entreprises.
États-Unis	Access America, Electronic Buying and Paying for the Federal Government, Framework for Global Electronic Commerce, Electronic Grants business plans	➢ FirstGov : Portail gouvernemental basé sur les intérêts. ➢ Access America for Students: Un portail informationnel et de services fournissant un point unique d'accès pour les étudiants. ➢ Votation en ligne (Arizona)
France	Programme d'action gouvernemental pour la société de l'information (PAGSI)	➢ Télédéclaration et télépaiement de la TVA ➢ Déclarations de résultats des entreprises et déclarations mensuelles d'échanges de biens

Pays, province ou état	Plan de transformation	Exemples de PES
Hong Kong	Digital 21 – Information Technology Strategy	➢ Recherche de copies de certificats de naissance, de mariage et de décès. ➢ Renouvellement d'un permis de conduire ➢ Création d'une entreprise (enregistrement, informations sur le financement, etc.)
Ontario	---	➢ Ontario Parks : Réservation d'emplacement dans les terrains de camping de la Province. ➢ Publications Ontario Online : Achat de publications
Singapour	Electronic Commerce Master Plan	➢ eCitizen Center : un portail orienté vers les étapes de vie et les activités des citoyens et entreprises ➢ Obtention de permis ➢ Inscriptions scolaires

La sécurité et la confidentialité des informations étant des éléments importants de toute stratégie de PES, ces différents pays ont mis en place des assises juridiques, organisationnelles et technologiques permettant de les garantir. Les sections qui suivent décrivent certaines initiatives ayant été développées dans ce sens.

1.2.2.1 Dimension juridique

Les diverses lois et projets de loi présentés à la section 1.2.1.1 couvrent aussi pour la plupart la fonction publique des divers pays. Elles visent à favoriser l'avancement du commerce électronique en faisant en sorte que les transactions et informations échangées électroniquement ne fassent pas l'objet de discrimination.

1.2.2.2 Dimension organisationnelle

Tel qu'affirmé dans la section 1.2.1.2, la définition d'un cadre de gestion de la sécurité est primordial au processus de dispensation des services électroniques. Il permet de structurer, d'orienter, de gérer et de mesurer la sécurité et ainsi de garantir la disponibilité et l'intégrité des infrastructures technologiques, des applications et des informations numériques, en plus de garantir la confidentialité de ces dernières lorsque requise. Les pays impliqués sérieusement dans des processus de PES partagent tous cette vision et se sont consacrés au développement de politiques, directives et standards de sécurité de la PES ou des technologies de l'information en général.

L'Angleterre a par exemple développé des politiques (et projets de politiques) couvrant les éléments suivants :

- **Sécurité** : La politique de sécurité vise à aligner les pratiques du e-gouvernement britannique avec les meilleures pratiques de sécurité du commerce électronique. Elle s'applique à tout le secteur public et à tous les canaux de distribution des services. Des travaux sont en cours pour ajouter à cette politique des thématiques telles que la confidentialité de l'information, la sécurité des services d'affaires et les besoins de protection des réseaux ;

- **Authentification**: La politique et les guides d'authentification établissent une approche commune d'authentification pour les départements, agences et autres organismes du secteur public ;
- **Métadonnées** : Des travaux sont en cours pour l'établissement d'une politique de métadonnées pour le e-gouvernement britannique ;
- **Carte à puce** : La politique de carte à puce fournit des standards et règles pour faciliter l'interopérabilité. Elle fournit aussi des conseils sur les problématiques d'acquisition ;
- **Confidentialité** : Le White Paper « Modernising Government » encourage fortement le gouvernement britannique à se soucier de la confidentialité. Ce document (il ne s'agit pas d'une politique) met en évidence les éléments clés de la confidentialité en rapport avec le e-gouvernement.

1.2.2.3 Dimension technologique

La création d'une AGSIN (dérivée d'une architecture d'entreprise gouvernementale), de même que le développement et la mise en œuvre de solutions de sécurité de toutes sortes, ont fait l'objet de travaux intenses depuis quelques années partout à travers le monde. Ainsi, dans un contexte général d'architecture d'entreprise gouvernementale, plusieurs agences fédérales et états américains ont élaboré des architectures de sécurité. Par exemple, c'est le cas des états de la Caroline du Nord et de l'Ohio et du département de la Défense. La communauté européenne de son côté a entrepris des travaux importants d'architecture visant l'échange de données entre les différentes administrations. L'architecture IDA (« Interchange of Data Between Administrations ») contient plusieurs éléments portant sur la sécurité, dont des orientations générales, un manuel technique et un document de base traitant spécifiquement de la sécurité de l'information numérique[13]. Ce dernier est un instrument didactique décrivant avec moult détails les « problèmes de sécurité pouvant survenir lors de la mise en œuvre d'un service transeuropéen basé sur une architecture commune bien définie ».

Ces différentes initiatives architecturales gouvernementales, en particulier les travaux de la Caroline du Nord, ont influencé de façon importante les pratiques gouvernementales, et même les pratiques de l'industrie un peu partout à travers le monde. La réalisation de l'AGSIN s'inspire d'ailleurs en partie de ces initiatives.

1.2.3 Gouvernement du Québec

Cette section présente le contexte gouvernemental québécois au niveau juridique, organisationnel et technologique. De plus, elle présente l'état actuel de la situation en matière de sécurité dans les ministères et organismes consultés, les chantiers centraux et les infrastructures centrales, de même que leurs principaux besoins en matière de sécurité. Cet état de situation couvrira aussi les dimensions juridique, organisationnelle et technologique.

1.2.3.1 Dimension juridique

L'AGSIN a pour principal but de mettre en place une solution de sécurité de l'information numérique et des échanges électroniques reposant sur le respect des critères de DICAI de la « Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale ». Cependant, la mise en œuvre de cette architecture doit aussi rencontrer des critères organisationnels, humains, technologiques et juridiques afin de maintenir le haut niveau de sécurité recherché. Pour éviter

[13] On se référera aux documents *Orientations pour l'architecture IDA, 1ère, 2ème et 4ème partie* pour plus de détails.

que les services électroniques perdent leur efficacité, leur valeur légale face aux tiers et leur force probante en cas de litige, il s'avère primordial de dresser le tableau des impacts juridiques et légaux liés à la mise en œuvre de l'architecture de sécurité gouvernementale.

Les critères de D-I-C-A-I de la Directive sur la sécurité

Les critères de DICAI (disponibilité – intégrité – confidentialité – authentification – irrévocabilité), présentés dans la « Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale », sont des assises importantes de la sécurité dans les affaires électroniques.

Le rôle des critères de DICAI à l'intérieur de l'AGSIN est décrit plus en détails aux sections 2.3 et 2.6.

Le cycle de vie de l'information

Après avoir reconnu l'importance des critères de DICAI de la Directive sur la sécurité, il faut aussi reconnaître l'importance du maintien de ces critères dans chacune des étapes du cycle de vie de l'information.

La relation entre le cycle de vie de l'information et l'AGSIN est décrite plus en détails aux sections 2.3 et 2.6.

La protection des renseignements personnels et de la vie privée

La protection des renseignements personnels et de la vie privée est un sujet de grande importance dans tout projet de sécurité lié aux affaires électroniques, et par le fait même du projet d'AGSIN. Les principales notions[14] qu'il faut considérer en regard de ce domaine de droit sont la responsabilité, la détermination des fins de la collecte de renseignements, le consentement, la limitation de la collecte, la limitation de l'utilisation, de la communication et de la conservation, l'exactitude, les mesures de sécurité, la transparence, l'accès aux renseignements personnels et la possibilité de porter plainte à l'égard du non-respect des principes.

Ces règles pourront par exemple faire référence dans le cadre de l'AGSIN à la responsabilité de l'autorité de certification à la suite de la diffusion non autorisée d'un renseignement à caractère nominatif ou à la publication de renseignements personnels dans un répertoire sans le consentement de la personne concernée.

Le respect de la législation et des sources de droit en vigueur

Le respect de la législation en vigueur est un élément majeur dans la validité d'une architecture et d'infrastructures de sécurité mises en œuvre. L'essentiel des sources de droit touchant l'AGSIN ou toute autre architecture de sécurité de l'information numérique (ASIN) se répertorie comme suit :

[14] Principes figurant en annexe de la loi C-6 fondés sur le Code type sur la protection des renseignements personnels de la CSA International, reconnu à titre de norme nationale (canadienne) en 1996. La loi C-6 est décrite plus en détails à la section 2.4.1.1

- la législation générale en vigueur aux niveaux provincial et canadien (codes, lois, règlements, décrets, tarifs, arrêtés en conseils, etc.) ;
- la législation sectorielle ;
- les lois cadres (la Loi sur les archives par exemple) ;
- les exigences contractuelles et conventionnelles.

Bien que la liste qui suit ne soit pas exhaustive, elle a l'avantage de dresser un portrait assez précis de la législation pouvant affecter de près ou de loin le projet d'AGSIN ou de toute ASIN. Ces lois sont d'ordre général et sont applicables à tous :

- Code civil du Québec (C.C.Q.)
- Loi sur les archives (L.R.Q., ch. A-21.1)
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., ch. A-2.1)
- Loi sur la protection des renseignements personnels dans le privé (P-39.1)
- Loi sur la protection des renseignements personnels et les documents électroniques (C-6)[15]
- Lois sur les droits d'auteurs (L.R. 1985, ch C-42) et les marques de commerce (L.R. 1985, ch T-13)
- Loi sur l'administration publique (PL 82)
- Charte des droits et libertés de la personne (C-12) et Charte canadienne des droits et libertés
- Loi concernant le cadre juridique des technologies de l'information (PL 161)
- Lois sectorielles

Ces lois sont décrites plus en détails à la section 2.4.1.1 du présent document.

Autres considérations d'ordre juridique

En regard du projet d'AGSIN et des projets d'ASIN et de PES, il s'avère important de regarder tout le contexte juridique qui doit s'appliquer. Un nombre important d'ajouts et de modifications devront être apportés au contexte juridique en place. Ces ajustements nécessiteront des efforts considérables qui devront être évalués et comptabilisés.

Les contrats et conventions sont aussi des sources de droits et d'obligations qui devront nécessairement faire l'objet d'une étude plus détaillée. Ainsi, il faudra revoir les ententes contractuelles déjà en vigueur avec les partenaires d'affaires, revoir les contrats ou demandes d'adhésion déjà utilisées, prévoir lorsque requis des clauses de non-responsabilité ou de responsabilité spécifique. Les ententes avec les fournisseurs de services devront aussi faire l'objet d'une analyse (responsabilités qui leur incombent et maintien du niveau de sécurité requis).

[15] La loi C-6, qui aura certains impacts au Québec, est décrite plus en détails à la section 2.4.1.1.

1.2.3.2 Dimension organisationnelle

Avant d'aborder la dimension technologique, il est essentiel dans un premier temps de faire un rappel de la démarche générale gouvernementale en matière de sécurité et de donner un aperçu des principales initiatives en sécurité réalisées par la Direction des politiques de gestion des ressources informationnelles (DPGRI) du SCT afin de situer le contexte global de cette intervention (AGSIN).

Politique québécoise de l'autoroute de l'information

Le Conseil des ministres, par des décisions datant du 2 août 1995 et du 26 janvier 1996, a confié au Secrétariat de l'autoroute de l'information (SAI) le mandat d'élaborer une stratégie québécoise de mise en œuvre de l'autoroute de l'information. En ce qui a trait plus spécifiquement à l'appareil gouvernemental, ces décisions précisent que le SAI doit concrétiser l'implantation des inforoutes au Québec par la mise en oeuvre d'un plan d'action et la mise en place de mécanismes efficaces de coordination des actions gouvernementales. Il doit aussi veiller à ce que le secteur public agisse en tant qu'usager modèle de l'inforoute. Un comité de coordination a été constitué par le SAI aux fins de la préparation d'un plan d'action pour la mise en œuvre de l'inforoute gouvernementale. Adoptée et rendu publique en 1998, la politique québécoise de l'autoroute de l'information sous le titre « Agir autrement » précise que cinq priorités ont été retenues : généraliser l'utilisation de l'inforoute de l'information, préparer la jeune génération à l'univers de la nouvelle technologie, bâtir un tronçon de l'inforoute qui reflète la culture québécoise, accélérer la transition de l'économie et la croissance de l'emploi et rapprocher l'État du citoyen et des entreprises.

L'élaboration d'une infrastructure à clés publiques gouvernementale (ICPG) et d'une politique québécoise de cryptographie et d'identification électronique (PCIE) s'inscrit à l'intérieur de la Politique québécoise de l'autoroute de l'information. Plus spécifiquement, ces travaux découlent des mesures 4.8, 4.9 et 4.10 de cette politique. Le projet d'ICPG sera traité plus loin dans ce document. De son côté, le projet de PCIE a plutôt résulté dans l'ajout des éléments pertinents à la loi concernant le cadre juridique des technologies de l'information approuvée par l'Assemblée nationale en juin 2001.

Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale

Guidées par ce plan d'action, les initiatives actuelles du Sous-secrétariat à l'inforoute gouvernementale et aux ressources informationnelles (SSIGRI) du SCT en matière de sécurité des ressources informationnelles portent principalement sur la « Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale ». Le SSIGRI du SCT travaille également avec le MRCI à développer des orientations et des outils visant la protection des renseignements personnels dans le cadre des nouveaux processus d'affaires.

En vue d'actualiser la « Directive concernant la sécurité de l'information électronique et des actifs informationnels » du 20 avril 1993, des travaux ont été amorcés voilà environ trois ans. La nouvelle directive, appelée « Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale », est en vigueur depuis le 23 novembre 1999 et a pris effet le 4 février 2000.

La nouvelle directive énonce des principes directeurs à appliquer, identifie les intervenants concernés par la gestion de la sécurité, détermine les responsabilités des ministères et des organismes et prévoit l'instauration des mécanismes de coordination et de collaboration appropriés en vue de prendre en compte

les critères de DICAI. Son implantation progressive va se réaliser dans le cadre d'un plan d'action en cours de réalisation.

La sécurité de l'information numérique comporte plusieurs domaines qui se recoupent. La nouvelle directive porte essentiellement sur le domaine de la sécurité de l'information numérique notamment les critères de DICAI. Les autres domaines seront éventuellement couverts par d'autres mesures comme l'indique, entre autres, le projet envisagé concernant la protection des renseignements personnels.

La directive touche l'ensemble des projets et des systèmes des M/O. Elle fait notamment obligation de nommer un responsable de la sécurité de l'information numérique (RSIN), d'établir un plan global de sécurité, de procéder à une évaluation périodique des risques, de produire annuellement au SCT des bilans et états de situation ainsi que plusieurs autres mesures.

Projets de support à la directive

Le SCT travaille actuellement[16] sur plusieurs projets pour faciliter l'application de la nouvelle directive, soit:

- **Projet de catégorisation de l'information numérique** : Ce projet vise à définir des catégories d'information numérique et les exigences de sécurité pour ces dernières. Un guide a été élaboré à cet effet en 2000, soit le « Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité » Des projets pilotes ont été complétés en décembre 2000 afin de tester ce guide. Le SSIGRI du SCT procède actuellement à certains ajustement et prévoit que le guide sera diffusé en juin 2001.
- **Projet sur les meilleures pratiques en matière de sécurité** : Ce projet vise à fournir aux ministères et organismes des renseignements pour guider leurs actions en sécurité. Actuellement un certain nombre de guides sont en cours de rédaction incluant notamment la « Pratique relative à l'utilisation d'Internet » et un « Recueil des pratiques recommandées, Partie 1 – Gestion de la sécurité ».
- **Projet de mise au point d'une méthode d'analyse de risques** : Ce projet vise à rechercher une méthodologie d'analyse de risques en fonction du contexte gouvernemental québécois afin d'assister les M/O dans ce domaine. Plusieurs méthodologies basées sur des normes et standards reconnus sont en cours d'évaluation ou ont été évaluées, dont notamment EBIOS, IPK, Marion, MEHARI, COBRA, COBIT 3.
- **Projet de mise en place d'un réseau d'expertise et de vigie** : Ce projet vise à mettre en place un réseau d'échange entre les responsables de la sécurité de l'information numérique afin de partager des connaissances et de s'entraider mutuellement, à l'aide par exemple d'un site Web sécurisé. Ce site est planifié pour l'automne 2001. Suivront par la suite des services de vigie, de prévention et détection d'intrusions ainsi que de soutien à la résolution de problèmes.
- **Projet d'amélioration des compétences en sécurité au gouvernement** : Ce projet vise à définir une stratégie pour améliorer les compétences en sécurité au gouvernement. Les travaux réalisés jusqu'à ce jour ont permis d'élaborer quatre cours de formation intitulés « Gestion de la sécurité », « Protection des renseignements personnels & les T.I. », « Aspects juridiques des technologies de l'information » et « Vérification informatique dans un environnement de travail électronique » Ces cours ont débutés en février 2001.

[16] Rappelons que les termes «actuellement », «en date du », «sont en cours », «sont envisagés», «jusqu'à ce jour », «sont réalisés » utilisés dans ce document présentent des informations en date de mai 2001.

- **Projet de bilan gouvernemental** : Ce projet consiste à élaborer un guide et des outils nécessaires pour effectuer le bilan de sécurité requis par la nouvelle Directive. Ces travaux sont réalisés en collaboration avec IBM et sont basés sur les dix domaines de sécurité tels que préconisés dans la norme BS7799[17].

Rapport d'un groupe de travail gouvernemental sur la sécurité de l'information

Toujours dans le cadre des travaux entourant la gestion de la sécurité de l'information numérique dans l'administration québécoise, un groupe de travail gouvernemental sur la sécurité de l'information a déposé en avril 1999 un rapport qui établissait les défis de gestion de la sécurité de l'information numérique. Ces défis incluent :

- Assurer la coordination de la sécurité de l'information numérique dans un environnement ouvert ;
- Assurer la cohérence des mesures de sécurité ;
- Accroître la capacité d'intervention des organisations ;
- Optimiser l'utilisation des ressources et des expertises ;
- Sensibiliser les employés à la valeur de l'information ;
- Assurer la gestion stratégique de la sécurité.

De plus, ce rapport proposait un cadre de gestion de la sécurité de l'information numérique en précisant les objectifs de ce dernier en plus de fournir une brève description et de décrire brièvement les rôles et responsabilités des principaux intervenants, soit le secrétariat du Conseil du trésor, le comité gouvernemental permanent sur la sécurité de l'information, les ministères et organismes, les services partagés et collectifs et le réseau d'expertise et de vigie.

Les recommandations de ce rapport ont été ou sont en voie d'être mises en place.

1.2.3.3 Dimension technologique

Avant d'aborder en détails les différents chantiers centraux, il est essentiel dans un premier temps de faire un rappel des différentes composantes physiques et solutions technologiques de sécurité pouvant garantir les critères de DICAI de la Directive sur la sécurité tout au long du cycle de vie de l'information dans le cadre de la PES protégée et des activités normales de l'État. Nous avons regroupé les différentes composantes physiques et solutions technologiques de sécurité en deux grandes catégories :

- Mécanismes pour assurer la protection, la détection et la correction
- Mécanismes pour assurer les critères de DICAI

Essentiellement, les différents mécanismes de sécurité et solutions technologiques dont il est question dans la première catégorie visent à mettre en place des mesures pour assurer la protection, la détection et la correction dans une démarche d'assurance de la sécurité. Ces technologies, outils ou services, décrits plus à fond à la section 2.5 et à l'annexe B, incluent notamment :

[17] On consultera la description de la norme ISO/IEC 17799 à l'annexe D pour plus de détails sur cette norme. Le Québec n'a pas adopté cette norme mais s'en est inspiré dans la conception d'un guide d'évaluation des risques.

- Technologies de coupe-feu ou de garde-barrière ;
- Technologies de réseau virtuel privé ;
- Outils ou services d'analyse de vulnérabilités ;
- Outils ou services de détection des intrusions ;
- Outils ou services de surveillance ;
- Outils ou services de journalisation et conciliation des journaux ;
- Outils ou services de gestion de la sécurité ;
- Outils ou services de garantie de haute disponibilité.

La seconde catégorie regroupe les différents mécanismes de sécurité et solutions technologiques visant à assurer les critères de DICAI tout au long du cycle de vie de l'information dans le cadre de la PES protégée et des activités normales de l'État.

Ces outils ou services, qui sont également présentés plus en détails à la section 2.5 et à l'annexe B, incluent principalement :

- Outils ou services associés à l'ICP ;
- Outils ou services associés au répertoire ;
- Outils ou services d'ouverture de session simplifiée ;
- Outils ou services d'authentification ;
- Outils ou services de contrôle des accès ;
- Outils ou services de chiffrement ;
- Outils ou services de contrôle d'intégrité.

Tel que nous le verrons dans les trois sections suivantes, un certain nombre de ces mécanismes de sécurité et solutions technologiques sont utilisés à l'intérieur des différents chantiers centraux, M/O et infrastructures centrales du gouvernement du Québec.

1.2.3.4 Chantiers centraux

Cette section présente les différents chantiers centraux ayant des liens directs avec la sécurité qui ont été identifiés et qui sont actuellement en cours au gouvernement du Québec afin d'offrir aux M/O des infrastructures de sécurité ayant un potentiel de mise en commun, de partage et de réutilisation. Ces chantiers incluent l'ICPG, le répertoire gouvernemental, la carte santé, SERTIR, GIRES et le serveur de paiement. Les pages qui suivent établissent un portrait global de ces chantiers centraux, de même que certains de leurs besoins en matière de sécurité.

ICPG

L'élaboration de l'infrastructure à clés publiques gouvernementale (ICPG) s'inscrit à l'intérieur de la Politique québécoise de l'autoroute de l'information. Plus spécifiquement, ces travaux découlent de la mesure 4.10 de cette politique.

Une infrastructure à clés publiques (ICP) concerne un ensemble d'acteurs, de pratiques et de technologies dédiés à la gestion de clés et de certificats de chiffrement (passeports et visas électroniques) permettant à des individus de se reconnaître à distance, d'effectuer en toute sécurité des transactions électroniques et d'échanger de l'information numérique de nature délicate.

L'ICPG, dont l'institution a été autorisée par le Conseil du trésor le 29 juin 1999, vise donc à répondre à ces besoins en garantissant, par l'usage de certificats et de la cryptographie, l'intégrité et la confidentialité de l'information numérique, l'authentification des utilisateurs et l'irrévocabilité des documents qu'ils rédigent et des actions qu'ils posent. Son implantation est en cours conformément au modèle fonctionnel approuvé par le Conseil du trésor.

L'objectif exprimé lors de la décision de juin 1999 était de faire en sorte que, progressivement, d'ici 2004, les employés de l'État dont les fonctions impliquent une interaction avec des données confidentielles ou la nécessité d'authentifier leur identité ou celle de leurs interlocuteurs, disposent d'un passeport et des visas électroniques nécessaires pour transiger avec des clientèles disposant de passeports et de visas électroniques équivalents. Dans le but de favoriser l'atteinte de cet objectif, un certain nombre de travaux ont été menés :

- **Politique de certificats** : le 31 mars 1999, le SCT a produit la version 3.0 du projet de politique de certificats intitulé « Document de travail sur la gestion de clés et de certificats au gouvernement du Québec ». La version 4 de ce document, résultat d'une consultation avec les gestionnaires de clés et certificats et les gestionnaires de l'infrastructure opérationnelle désignés par le Conseil du trésor, sera présentée pour adoption à ce dernier au cours de l'année 2001 sous forme de directive.
- **Modèle fonctionnel d'une infrastructure à clés publiques gouvernementale** : En juillet 2000, ce rapport est présenté au SCT. Le but de ces travaux est de définir un modèle interopérable qui permet la cohabitation de solutions provenant de différentes autorités de certification et de différents fournisseurs. Il vise à compléter le rapport intitulé « Document de travail sur la gestion de clés et de certificats au gouvernement du Québec » dans sa version 3.0 du 31 mars 1999, issu du SCT. Le but de ce document est d'exposer les différentes fonctionnalités d'une infrastructure à clés publiques afin de servir de modèle à une infrastructure à clés publiques gouvernementale. Ce document repose sur des standards qui permettent une interopérabilité entre les ICP, et non sur les applications des fournisseurs d'ICP. Ce document, qui se situe en amont d'une politique de certification, identifie l'ensemble des éléments à prendre en compte lors de la conception de l'ICPG.
- **Bilan des projets et impact des infrastructures à clés publiques** : Ces travaux, dont le rapport a été présenté en mars 2000, a pour objectif de tracer un bilan réaliste des projets des ministères et organismes, en cours ou à venir, avec un potentiel d'utilisation de l'ICPG ou de tout autre moyen de sécurisation des accès électroniques des employés et des clientèles du gouvernement. Ce rapport présente les résultats de l'analyse et un certain nombre de recommandations afin d'éclairer le SCT dans ses prises de décision relativement à un positionnent gouvernemental face à l'ICP, à l'établissement d'une ICPG et la mise en place du concept de « Certificat Québec »
- **Projet « Certificat Québec »** : Dans le cadre de ce projet, le SCT a mis sur pied un groupe de travail pour la définition de la ou des normes sur la délivrance et la gestion de clés et de certificats pour sécuriser les transactions électroniques au sein du gouvernement, ainsi qu'entre le gouvernement et les individus/entreprises du Québec. Ce groupe de travail a pour mandat global de remettre au Conseil du trésor un rapport de conception du certificat normalisé afin d'appuyer le démarrage des travaux du comité de normalisation qui sera piloté par le Bureau de Normalisation du Québec.
- **Désignation de la Direction générale des services de justice du ministère de la Justice comme gestionnaire de clés et certificats** : Dans l'exercice de ses fonctions de gestionnaire des encadrements administratif et technique, le Conseil du trésor a désigné, le 27 février 2001, la Direction générale des

services de justice du ministère de la Justice comme gestionnaire de clés et certificats afin de répondre aux besoins de certification des employés, dispositifs et applications de l'État et des mandataires du gouvernement ou de ses clients, à condition que la vérification d'identité soit faite, lors d'une entrevue, par un Agent de vérification de l'identité (AVI) autorisé par le SCT. D'ici le 7 octobre 2003, le MJQ agira également comme gestionnaire des infrastructures opérationnelles permettant de répondre à ces besoins de certification des ministères et organismes. À partir du 7 octobre 2003, le SSSG prendra la relève de la partie assumée par le MJQ comme gestionnaire des infrastructures opérationnelles.

- **Désignation du SSSG comme gestionnaire de clés et certificats et des infrastructures opérationnelles** : Dans l'exercice de ses fonctions de gestionnaire des encadrements administratif et technique, le Conseil du trésor a désigné, le 27 février 2001, le SSSG comme gestionnaire de clés et certificats et des infrastructures opérationnelles dans les cas où le MJQ n'est pas en mesure de délivrer des clés et certificats dans un contexte particulier et dans les cas où l'identification des usagers est établie par le M/O. À partir du 7 octobre 2003, le SSSG cessera d'être un GCC pour se concentrer sur ses fonctions de GIO.
- **Sélection d'un ou de plusieurs produits d'ICP (à venir) :** Le ou les produits d'ICP retenus serviront à émettre et à gérer les certificats des clientèles gouvernementales.

L'ICPG (et toute ICP en général) se doit elle-même d'être protégée afin d'offrir un niveau adéquat de disponibilité, d'intégrité et de confidentialité des informations numériques emmagasinées, traitées et échangées lors des communications avec le serveur de clés et de certificats. De plus, l'authentification des utilisateurs habilités au niveau approprié et le cas échéant, l'irrévocabilité des communications entre l'utilisateur et le serveur de clés et de certificats devront être garantis.

Dimension juridique :

La loi concernant le cadre juridique des technologies de l'information amènera des obligations qui se traduiront en besoins de sécurité organisationnels et technologiques en ce qui a trait à l'utilisation du répertoire pour rendre public les certificats de chiffrement. À cet effet, la loi contient des dispositions pour baliser la prestation de services de certification et de répertoire et offre à tout prestataire de services de certification, qu'il soit du Québec ou d'ailleurs, de se faire accréditer par une personne ou un organisme déterminé par le gouvernement en fonction des mêmes critères d'appréciation. La loi prévoit également les exigences à respecter pour assurer la valeur probante des documents électroniques et le lien entre une personne et le document qu'elle signe.

Dimension organisationnelle :

L'infrastructure à clés publiques nécessite une répartition adéquate des responsabilités entre les organismes exerçant des fonctions centrales, communes ou partagées. A cet effet, le modèle fonctionnel de l'ICPG établit le découpage requis. Il est donc primordial que les besoins en terme de sécurité administrative et organisationnelle ainsi que du personnel responsable de l'ICPG soient adressés par l'adoption d'une politique de certificats (par le GEAT) et l'établissement de pratiques et procédures de certification par les gestionnaires de clés et certificats désignés par le Conseil du trésor. De plus, des considérations importantes au niveau de la sécurité physique et du milieu de l'ICPG amèneront à intégrer dans la politique de certification des mesures spécifiques dans ce domaine. Les besoins au niveau de la sécurité opérationnelle sont également importants et devront se traduire notamment au niveau des procédures et des guides d'opération ainsi qu'au niveau des mesures de surveillance, de détection et d'urgence.

Finalement, un audit de sécurité permettrait d'établir un portrait exact de la situation en matière de sécurité des services de gestion des clés et certificats et de gestion de l'infrastructure opérationnelle de la DGT et

du RDPRM et d'évaluer les modifications éventuelles à y apporter dans le cadre de la solution permanente applicable après le 7 octobre 2003.

Dimension technologique :

Des besoins existent principalement au niveau de la normalisation de la paramétrisation et de l'administration sécuritaire de l'ICP ainsi que sur la mise en place et la gestion d'outils de prévention, de détection et de correction. De plus, des considérations importantes au niveau des acquisitions (ex. : normes techniques) et du cycle d'élaboration de systèmes (ex. : règles de développement d'interfaces) permettront de contribuer à l'interopérabilité de l'ICPG avec d'autres ICP.

Répertoire gouvernemental

L'origine de ce projet est la mesure 5.2 de la politique québécoise de l'autoroute de l'information. Celle-ci s'énonce ainsi : « Voir, de concert avec le ministère des Relations avec les citoyens et de l'Immigration, à mettre en place le répertoire gouvernemental québécois afin de permettre aux individus et aux entreprises d'avoir accès à la description des services offerts à la population, aux références concernant les documents gouvernementaux ainsi qu'aux coordonnées des employés de l'État; le répertoire électronique sera accessible dans le réseau Internet ».

Les objectifs du projet sont de définir le répertoire gouvernemental et de le mettre en œuvre. Trois fonctions principales sont associées à celui-ci : la localisation (décrire et repérer les objets), la garantie (gérer les identités certifiées et les autorisations) et le partage (soutenir le partage des objets et de leurs divers attributs). Le principe général que l'on tend à promouvoir avec le répertoire est de chercher à intégrer l'existant plutôt que de procéder à une reconstruction.

Afin d'atteindre ces objectifs, le SCT publiait en décembre 1997 un rapport intitulé « Conception détaillée du répertoire gouvernemental » ayant pour objet de situer le répertoire gouvernemental dans le contexte du déploiement de l'inforoute et d'illustrer sommairement certaines fonctionnalités. Ce document présente : la vue générale du répertoire gouvernemental, l'architecture du service de répertoire, l'appellation et la structure de l'arborescence du répertoire, les mécanismes de sécurité et leur architecture et le schéma du répertoire gouvernemental. On fait état dans ce document de tous les objets à l'intérieur de l'appareil gouvernemental que l'on veut localiser, garantir et partager. À titre d'exemples, on y retrouve : les personnes, les unités organisationnelles, les documents, les entités d'application, etc.

La conception du répertoire gouvernemental est sous la responsabilité du SSIGRI du SCT. La DGT assume la réalisation du répertoire alors que la DGSIG apporte un soutien en matière de modélisation des données.

En ce qui concerne les éléments actuellement en place et prévus, on retrouve :

- Au niveau de la fonction localiser, l'utilisation initiale du répertoire est prévue pour la localisation des employés du gouvernement. Un répertoire gouvernemental partiel des employés du gouvernement est actuellement en hébergement à la DGT. Cette fonction utilise un sous-ensemble de ce répertoire pour donner l'accès aux pages blanches (équivalent au bottin de téléphone) aux employés eux-même via l'intranet gouvernemental et éventuellement aux individus via Internet.
- Au niveau de la fonction garantir, l'utilisation du répertoire est prévue initialement pour fins d'identification et d'authentification ainsi que pour le contrôle des accès des employés du gouvernement devant être connus sur le réseau. À cet effet, le répertoire gouvernemental devient une des pièces maîtresse de l'AGSIN. Il est prévu que le répertoire gouvernemental soit alimenté et

continuellement mis à jour par GIRES. Il est également prévu que la fonction garantir s'appuie sur les résultats du chantier de l'ICPG.

- Au niveau de la fonction partage, deux interventions additionnelles en relation avec le répertoire gouvernemental ont été initiées :

  - **le registre de métadonnées** : Un premier sous-ensemble a été établi selon la norme XML définissant plusieurs profils de métadonnées pour la prestation électronique de service. Il s'agit notamment du document de transaction, du tableau des autorisations, et de l'étiquette de signature numérique. Ces profils seront intégrés sous peu au répertoire gouvernemental actuellement hébergé à la DGT.
  - **l'ingénierie documentaire** : Actuellement une collection de 13 documents a été publiée. Chacun d'eux expose une problématique particulière au document électronique et suggère des solutions, des normes et des règles pour répondre aux besoins des organisations.

  Il est important de retenir qu'en matière de sécurité de l'information numérique, il existe une relation étroite entre le répertoire, le registre de métadonnées et l'ingénierie documentaire et que l'AGSIN doit en tenir compte (ex. : les classes XML (schémas) sont définies dans le registre de métadonnées, les instances de classe sont incluses dans le répertoire, etc.). Le SSIGRI du SCT établit actuellement une stratégie afin de compléter un plan d'action pour l'élaboration d'un guide de gestion des documents afin d'assister les M/O.

Il n'y a pas pour l'instant de stratégie et de planification d'ensemble pour la poursuite des travaux liés au Répertoire Gouvernemental. Les travaux relatifs à ce dernier s'exécutent actuellement selon une approche expérimentale.

Le répertoire gouvernemental vise à répondre aux besoins de décrire et repérer les objets, de gérer les identités certifiées et les autorisations en plus de soutenir le partage des objets et de leurs divers attributs. Parmi les objets prévus au répertoire, on retrouve les certificats de chiffrement (passeports et visas électroniques) des employés de l'état. Dans cette mesure, il se doit lui-même d'être hautement protégé afin de garantir la disponibilité, l'intégrité et la confidentialité des informations numériques emmagasinées, traitées et échangées lors des communications. De plus, l'authentification des utilisateurs habilités au niveau approprié et le cas échéant, la non-répudiation des communications entre l'utilisateur et le répertoire pourront être garanties. Plus spécifiquement, les besoins suivants devront être considérés :

Dimension juridique :

Tout comme pour l'ICPG, la loi concernant le cadre juridique des technologies de l'information amènera des obligations qui se traduiront en besoins de sécurité organisationnelle et technologique en ce qui a trait à l'utilisation du répertoire pour rendre public les certificats de chiffrement. À cet effet, les articles 22, 46, 48, 50, 52, 54, 55, 60, 61 et 63 touchent plus particulièrement le répertoire. Les obligations relatives à l'utilisation du répertoire pour la publication des certificats de chiffrement devront être garanties par l'organisme responsable du répertoire gouvernemental. De plus, dépendant de la nature des informations numériques emmagasinées, traitées et échangées sur le répertoire, d'autres lois pourraient également préciser des éléments additionnels à considérer.

Dimension organisationnelle :

Le responsable du dossier au SCT remarque un niveau d'imprécision au point de vue de l'organisation, de sorte que les responsabilités ne sont pas toutes bien définies ni assumées. La gestion du répertoire nécessitera de définir et de confier un certain nombre de responsabilités de nature commune à un

organisme central. Tout comme dans le cas de l'ICPG, il est primordial que les besoins en terme de sécurité administrative et organisationnelle ainsi que du personnel responsable du répertoire soient adressés de manière précise et se reflète dans un cadre de gestion du répertoire gouvernemental clairement défini. Il en va de même au niveau de la sécurité physique et du milieu ainsi qu'au niveau de la sécurité opérationnelle.

Dimension technologique :

Les mêmes considérations qu'au niveau de l'ICPG s'appliquent au répertoire en tant que support privilégié des certificats de chiffrement.

SERTIR

Le SERTIR (Services transactionnels d'information et de repérage), un serveur WEB de données et d'applications développé par la DGSIG, est mis à la disposition des M/O qui veulent créer des services transactionnels et de commerce électronique. Les clients finaux des services mis en place à l'aide de SERTIR sont les individus, les entreprises et les employés de l'état. Plus spécifiquement, le SERTIR offre un ensemble de services communs favorisant la mise en place de la prestation électronique de services tels que des services transactionnels, des accès aux banques de données, des formulaires électroniques, des boutiques électroniques, des services de paiement, des services de repérage, des services d'abonnement, des accès contrôlés aux services et des infrastructures technologiques. En plus de ces services, la DGSIG offre des services conseils pour assister les M/O dans la préparation de plan d'affaires en affaires électroniques et dans le développement de services transactionnels utilisant les services du SERTIR.

Démarré en 1998, le projet SERTIR a été présenté officiellement aux M/O en octobre 1999 suite à la réalisation d'un certain nombre de travaux préparatoires tels que le développement d'une architecture technologique, la réalisation d'un plan d'affaires et d'une vitrine démontrant ses services. De novembre 1999 à mai 2000, des efforts importants ont été mis dans la documentation et la mise en place d'un environnement de développement et dans la conception des services transactionnels d'émulation terminale, d'accès aux BD, de paiement par carte de crédit (intégration de la solution du Ministère des Finances) et d'accès contrôlés aux services. Des infrastructures technologiques de laboratoire et de production ont aussi été mises en place.

La phase III du SERTIR consistera principalement à mettre en place et à déployer les autres services.

L'étude de certains documents relatifs au SERTIR et la consultation d'une personne ressource mettent en évidence un certain nombre de besoins technologiques en matière de sécurité. Ceux-ci sont relatifs à la disponibilité des applications, à l'authentification et l'habilitation des utilisateurs, à la sécurité due au chiffrement des données et à la prévention des intrusions. Notons entre autres :

Dimension organisationnelle :

Les responsables du SERTIR doivent prévoir un certain nombre d'éléments organisationnels et administratifs essentiels à la bonne marche des activités. Ainsi, dans un premier temps, des politiques, directives et procédures de sécurité doivent être développées spécifiquement dans le cadre du projet SERTIR. Peu de travaux, faute de financement, ont été faits dans ce sens.

Il est aussi très souhaitable que les responsabilités respectives des M/O et de la DGSIG relativement au projet SERTIR soient définies. Il a d'ailleurs déjà été établi que les contenus déposés sur le SERTIR sont la responsabilité des M/O alors que les infrastructures technologiques sont sous la responsabilité de la

DGSIG. De plus, la DGSIG prend en charge la sécurité de SERTIR du point de vue du contenant. Cependant, les M/O doivent obtenir l'accord de la CAI sur le contenu, les services et les applications qu'ils mettent en ligne sur Internet. De même, la définition des rôles et responsabilités des individus en matière de sécurité est nécessaire à la fois dans les M/O et à la DGSIG.

Du point de vue de la disponibilité des applications et informations numériques, bien que des moyens technologiques permettent de garantir une certaine disponibilité des infrastructures technologiques, applications et informations numériques, il est important d'accompagner ces solutions d'éléments organisationnels tels que des procédures de surveillance, un plan de relève, un plan d'urgence, etc. La DGSIG dispose de tels plans pour l'ensemble de ses infrastructures, y compris celles de SERTIR.

De plus, au niveau de la sécurité physique et du milieu, les infrastructures technologiques doivent être hébergées dans un centre où l'accès sera contrôlé. Cela fera donc en sorte que des mesures (carte disponible au personnel autorisé seulement, surveillance et service de gardiennage, température contrôlée, etc.) seront en place et ainsi d'un point de vue sécurité physique tous les équipements feront l'objet d'une protection. Ces besoins sont adressés par les services offerts par le centre de traitement de la DGSIG. Les équipements actuels du SERTIR sont dans ce périmètre sécurisé.

Dimension technologique :

Considérant les exigences importantes en terme de disponibilité des infrastructures technologiques, applications et données (24/7), il est essentiel de prévoir des mécanismes de sécurité et solutions technologiques qui la garantissent tels que des mécanismes de duplication et de redondance des infrastructures technologiques, des applications et de l'information numérique, le balancement de la charge, etc. La majorité de ces besoins sont comblés par la DGSIG. Cependant, bien que la DGSIG assure la disponibilité de ses infrastructures technologiques et applications, de même que des informations numériques stockées chez elle, elle n'assure pas celle des infrastructures, applications et informations numériques situées dans les M/O. Ces derniers devront fournir leurs propres mécanismes assurant la disponibilité et le respect des niveaux de services.

Des technologies telles qu'une zone libre sécurisée (zone démilitarisée - DMZ) entre Internet et le réseau interne de la DGSIG, des coupe-feu, un réseau hautement sécurisé protégeant les M/O, de même que des outils de détection d'intrusions doivent assurer la sécurité du réseau interne de la DGSIG, des réseaux des M/O, du serveur de paiement ainsi que des ordinateurs minis et centraux. La DGSIG et le gouvernement proposent déjà plusieurs de ces outils (DMZ, coupe-feu, RICIB). De plus, dans l'éventualité où des données sensibles sont échangées entre les postes clients sur Internet et les serveurs de la DGSIG, elles devront être chiffrées. Notons que c'est déjà le cas pour les applications actuellement en exploitation.

Les exigences d'authentification et d'habilitation doivent être adressées à l'aide d'un mécanisme de contrôle des accès. Cependant, considérant les différents profils des usagers qui utilisent les services dispensés par le SERTIR de même que les différents types d'informations numériques qui y circulent, il est impératif de prévoir des mécanismes qui permettent à la fois l'authentification faible et forte. Si le mécanisme qui est présentement en place (code d'utilisateur et mot de passe) convient parfaitement à certains types d'usages et de données, il n'est pas envisageable de l'utiliser dans toutes les circonstances.

Le SERTIR devra à court terme avoir recours à des technologies d'authentification fortes telles qu'une ICP (incluant un répertoire), des jetons d'authentification ou autres. Dans l'éventualité probable où le SERTIR aura recours à une ICP, il n'est pas possible, sans l'accord du Conseil du trésor, d'en développer une. Une infrastructure commune (l'ICPG) sera plutôt utilisée. Notons aussi que dans certaines situations (accès à des informations publiques par exemple), aucune authentification ne sera nécessaire. Les mécanismes mis en place doivent donc être suffisamment flexibles pour supporter ces trois alternatives.

Notons qu'en plus des mécanismes d'authentification et d'habilitation propres à SERTIR, les M/O fournissent aussi des mécanismes de ce type pour limiter l'accès aux systèmes accessibles à partir de SERTIR (et aux autres systèmes). Ces mécanismes sont cependant très hétérogènes, ce qui est peu acceptable du point de vue de l'utilisateur.

GIRES

Amenés par la loi sur l'administration publique à se pencher sur l'efficacité et la performance de leurs organisations, les M/O doivent se munir d'outils permettant une meilleure gestion de leurs ressources. C'est dans cette perspective que le Conseil du trésor a autorisé, en février 1999, le lancement d'un appel d'offres en vue d'acquérir un progiciel de gestion intégrée des ressources humaines, financières et matérielles. Avec l'aide des ministères et organismes, le gouvernement a arrêté son choix en juin 1999 sur le progiciel de la firme Oracle. Ce progiciel est appelé à non seulement remplacer deux systèmes dont les origines remontent au début des années 1970, soit SAGIP (Système automatisé de gestion des informations sur le personnel) et SYGBEC (Système de gestion budgétaire et comptable), mais aussi à introduire des facilités administratives axées sur les méthodes les plus modernes de gestion.

GIRES couvre l'ensemble des besoins en matière de gestion des ressources humaines, financières et matérielles du gouvernement et est destiné principalement à deux catégories d'utilisateurs :

- les utilisateurs réguliers qui sont chargés de la gestion des ressources de M/O. Ces utilisateurs ont accès à un plus grand nombre de services que les utilisateurs précédents ;
- les employés qui peuvent accéder aux fonctions de type libre service de GIRES et qui leur permet de compléter leur permis d'absence, rapports de dépenses, etc.

Les clientèles de la solution GIRES se composent de près de 66 000 utilisateurs répartis dans 156 ministères, organismes ou fonds spéciaux. Les utilisateurs réguliers sont estimés à 11 000, dont 3 875 gestionnaires.

Les besoins de GIRES en matière de sécurité s'apparentent à ceux de SERTIR puisque, comme ce dernier, les applications GIRES seront hébergées par la DGSIG. Cependant, comme GIRES servira à centraliser les données relatives aux ressources du gouvernement, et non simplement à aiguiller les requêtes, il est de la plus grande importance de lui accorder un très haut niveau d'attention et de protection.

Dimension juridique :

GIRES doit tenir compte des différentes lois et des différents règlements régissant l'administration publique, particulièrement la loi 82 sur l'administration publique, et de la loi concernant le cadre juridique des technologies de l'information. Notons que GIRES considérera l'opportunité et la pertinence de procéder à des ajustements du cadre réglementaire plutôt que de modifier les pratiques d'affaires éprouvées incluses dans le progiciel, bien que des assouplissements à cette politique sont probablement à prévoir.

Dimension organisationnelle :

D'un point de vue organisationnel, de nombreuses mesures devront être prévues. Celles-ci incluent :

- Des éléments encadrants tels que des politiques, directives et procédures de sécurité spécifiques à GIRES devront aussi être développées ;

- Une définition des responsabilités respectives des M/O et de GIRES en matière de sécurité de l'information est nécessaire. Des efforts importants ont déjà été consentis à ce niveau ;
- La définition des rôles et responsabilités en matière de sécurité est nécessaire à la fois dans les M/O et dans GIRES ;
- La mise en place d'un cadre de gestion de l'exploitation, de procédures de surveillance, d'un plan de relève, d'un plan d'urgence, etc. sont nécessaires ;
- Les infrastructures technologiques devront être hébergées dans un centre où l'accès sera contrôlé. Cela fera donc en sorte que des mesures (carte disponible au personnel autorisé seulement, surveillance et service de gardiennage, température contrôlée, etc.) seront en place et ainsi d'un point de vue sécurité physique tous les équipements feront l'objet d'une protection.

Dimension technologique :

GIRES doit se protéger contre les intrusions. Ainsi, il est prévu qu'il utilise les différents coupe-feu de la DGSIG. Afin de protéger le trafic, les échanges entre les postes de travail et les serveurs de GIRES seront cryptés et les transactions devront s'effectuer uniquement sur un réseau privé protégé de l'Internet. De plus, un accès à distance (RAS) à partir d'un modem ou un accès Internet sécurisé (RPV, par exemple) devra permettre aux utilisateurs en mode libre-service de se brancher de façon sécuritaire au réseau à partir de l'extérieur. Ces derniers besoins correspondent en partie aux services offerts par le RICIB et aux services qui seront offerts par le RETEM.

Il est aussi prévu que GIRES utilisera le chiffrement des messages et implantera la sécurité définie dans les applications Oracle pour authentifier et habiliter tous les utilisateurs avant de leur donner accès à GIRES, et ce, en fonction des droits d'accès qui leur ont été accordés. La méthode d'authentification supportée pour le moment est l'utilisation d'un code utilisateur et d'un mot de passe (authentification faible). Cependant, l'utilisation d'une méthode d'authentification forte est à l'étude. Deux méthodes sont étudiées, l'utilisation d'un jeton d'authentification ou d'un certificat. Dans ce dernier cas, il est nullement prévu que GIRES déploie sa propre ICP. Notons que l'utilisation d'une ICP se fera conjointement avec la fonction de sécurité de Oracle. Cette dernière est solide et doit être conservée.

Au niveau de la disponibilité, il est impératif qu'il soit hautement disponible en période d'exploitation puisqu'il sera le centre névralgique de la gestion des ressources au gouvernement du Québec. Des mécanismes aussi solides, si ce n'est plus solides que dans le cas de SERTIR devront être utilisés : mécanismes de duplication et de redondance des infrastructures technologiques, applications et informations numériques, balancement de la charge, outils d'exploitation pour assurer un suivi automatisé et serré de l'environnement, etc.

Dans une optique d'AGSIN, GIRES aura un rôle important. En effet, le répertoire gouvernemental est une des pièces maîtresse de l'AGSIN et il est prévu que GIRES l'alimente et le mette continuellement à jour.

Serveur de paiement :

L'extrait suivant, tiré de l'appel d'offres du ministère des Finances pour l'acquisition d'un service de paiement des transactions de vente de biens et service, permet de bien cerner les objectifs visés par le projet :

> *« Plusieurs ministères et organismes du gouvernement du Québec, en accord avec la politique gouvernementale sur l'autoroute de l'information, offrent ou offriront sous peu l'accès à leurs services via des réseaux publics ou privés. Considérant que certains de ces services nécessiteront*

le paiement de frais et/ou de droits, le ministère des Finances désire implanter un service permettant d'assurer l'encaissement des paiements pour les transactions gouvernementales réalisées via ces réseaux publics (Internet), privés et par l'inforoute gouvernementale. »

Le serveur de paiement, exploité par la Banque Nationale du Canada (BNC), est actuellement en service sous la dénomination de *P@iement en ligne* et supporte la gamme complète des transactions financières et administratives : paiement, annulation, remboursement partiel ou total, information de gestion, etc. Il est compatible avec la plupart des plates-formes de commerce électronique. Le serveur de paiement peut aussi bien accommoder les M/O disposant de leur propre site de commerce électronique ou partageant une infrastructure commune telle que SERTIR.

P@iement en ligne reconnaît les cartes de crédit Visa, MasterCard et American Express et les cartes acceptées sont déterminées par les M/O. D'autres modes de paiement seront progressivement ajoutés au rythme de l'évolution des moyens technologiques dont le paiement pré-autorisé Internet, le débit direct Internet et la monnaie électronique.

Les M/O utilisateurs du service *P@iement en ligne* sont le Directeur de l'État civil, les Publications du Québec, le ministère des Ressources naturelles, la Société des alcools du Québec, le SERTIR et le ministère des Transports du Québec.

Le cadre de gestion de la sécurité ainsi que l'architecture technologique du serveur de paiement en place sont ceux du fournisseur, c'est-à-dire de la BNC. Le serveur de paiement est hébergé dans une infrastructure certifiée par cette dernière. Pour des raisons évidentes de sécurité, le fournisseur ne peut dévoiler ces éléments. Toutefois, les normes et standards de sécurité du serveur sont les mêmes que celles édictées pour les opérations bancaires.

Les besoins en matière de sécurité suivants sont pris en compte :

- Confidentialité ;
- Intégrité des données ;
- Authentification de l'émetteur ;
- Non-répudiation de la transaction ;
- Formulaire protégé ;
- Chiffrement des informations véhiculées ;
- Autorisation des achats en temps réel et sans intervention humaine ;
- Solution souple et évolutive ;
- Sensibilisation et formation.

Les divers besoins immédiats et futurs relatifs à la sécurisation des transactions et des paiements, de même que des infrastructures du serveur de paiement semblent donc avoir été pris en compte par la BNC et le ministère des Finances.

1.2.3.5 Chantiers sectoriels

Carte santé

Le gouvernement québécois a approuvé, en septembre 1991, l'expérimentation sociale de la carte santé, afin d'en vérifier l'utilité et l'acceptabilité, en contexte réel d'utilisation, et d'en apprécier le potentiel de diffusion. La Régie de l'assurance maladie du Québec (RAMQ) a été désignée comme maître d'œuvre du projet.

Un premier projet expérimental de deux ans a été mené à Rimouski de 1993 à 1995. Ce projet consistait à expérimenter l'usage d'une carte à microprocesseur visant à rendre disponible, dans un délai raisonnable, de l'information clinique, habituellement dispersée dans divers points de services ou lieux de pratique et sur des supports disparates et ce, d'une façon confidentielle et sécuritaire. Les travaux effectués incluaient des opérations de recherche, de développement, d'implantation et d'évaluation.

Au printemps 1998, le ministère de la Santé et des Services sociaux mandatait la RAMQ pour réaliser un nouveau projet de démonstration sur trois ans de son système Carte santé. Sous la coordination de la Régie régionale de la santé et des services sociaux de Laval, la RAMQ expérimente, en collaboration avec le Centre hospitalier ambulatoire régional de Laval (CHARL), un nouveau système de carte santé à microprocesseur dans le cadre de la programmation régionale des services ambulatoires (PRSA). Ce projet a pour but de démontrer le potentiel de la carte à puce dans le domaine de la santé. Cette initiative résulte de la conjonction de deux entités distinctes : le système d'information qui supporte la Programmation régionale des services ambulatoires de Laval et le système de carte à microprocesseur.

L'originalité de cette approche réside dans la synergie qui sera déployée. Ainsi, le système d'information servira tout d'abord à alimenter le contenu d'un dossier carte santé (DCS), élément important du système de carte à microprocesseur. À son tour, la carte à puce sera utilisée comme outil ultime de sécurisation de l'accès au système d'information de la PRSA et de la circulation des données cliniques du DCS de l'usager entre les établissements de Laval et les intervenants participants.

Le projet PRSA - Carte santé s'intègre dans un projet plus large visant à démontrer l'interopérabilité de la carte à puce entre le Canada et trois pays européens déjà impliqués dans le projet NETLINK du G7, soit la France, l'Italie et l'Allemagne. Il constitue également la contribution du Québec au projet NETLINK.

Dans le contexte actuel et tant que l'usage définitif de la carte santé n'aura pas été défini, il ne sera pas possible d'exprimer les besoins en matière de sécurité de celle-ci. En effet, le 16 février 2001, la CAI a émis un avis confidentiel défavorable concernant la nouvelle orientation du gouvernement[18].

Cependant, la CAI ne s'oppose pas à l'utilisation d'une carte à puce dans la santé comme outil de protection des renseignements personnels si elle est associée au consentement de l'usager lors de la collecte et de la communication de l'information ainsi qu'à des mécanismes de signature électronique.

Lorsque le gouvernement du Québec aura clairement énoncé ses orientations sur l'utilisation définitive de la Carte Santé et que la Commission d'accès à l'information aura rendu un avis positif sur ces nouvelles orientations, il sera alors possible de formuler des besoins précis en matière de sécurité de l'information numérique dans ce domaine.

[18] Robert Dutrisac, *La CAI dit non au projet de carte-santé*, *Le Devoir*, 20 février 2001

1.2.3.6 M/O

Cette section présente un résumé de l'état de la situation des ministères et organismes en matière de sécurité en date du 23 février 2001. Cette image est principalement basée sur les commentaires et l'information recueillis suite à des ateliers d'échange menés en février et mars 2001 avec seize M/O [19] et aux cueillettes d'informations effectuées en février 2001 auprès de douze M/O représentatifs de la situation gouvernementale. Les résultats complets de ces cueillettes d'informations sont présentés à l'annexe C. La vision présentée n'est pas exhaustive mais donne une très bonne idée de la situation dans les M/O

Les constats suivants ont été faits :

Dimension juridique :

- Une grande majorité des M/O rencontrés indique que les lois et règlements applicables à ceux-ci (générales et/ou spécifiques) ne semblent pas adaptés à la PES ou aux échanges entre eux. Certains M/O ont effectué des demandes d'avis juridiques et sont en attente de réponses.

De plus, les cueillettes ont permis de mettre en évidence les enjeux et impacts juridiques suivants :

ENJEUX ET IMPACTS JURIDIQUES

Enjeux	Impacts
➢ Respect de lois et règlements ➢ Respect de la vie privée ➢ Échange et partage d'information numérique entre les M/O ou avec d'autres organisations ➢ Responsabilité des utilisateurs ➢ Gestion du consentement (consentement initial, consentement lors d'échanges d'informations personnelles entre M/O) ➢ Gestion de l'habilitation ➢ Authentification des individus ➢ Valeur légale des documents	➢ Modification des lois et règlements ➢ Modification aux contrats ➢ Analyses et avis juridiques ➢ Changement de culture (intégration papier/électronique)

La cueillette démontre clairement que les M/O sont confrontés à des lois et règlements qui ne sont pas, dans plusieurs cas, adaptés à un contexte de PES protégée. Il est donc essentiel que l'ensemble des lois et règlements régissant les M/O soit en harmonie avec le nouveau canal d'affaires que constitue la PES. La loi concernant le cadre juridique des technologies de l'information, entre autres, facilitera la reconnaissance légale des documents sur support informatique. Une révision des contrats et l'inclusion de clauses mieux adaptées à la PES sont également nécessaires dans plusieurs cas.

[19] ANQ, CSST, DGIGRI du SCT, DGSIG, DGT, MFQ, MJQ, MRCI, MRN, MRQ, MSS, MSSS, RAMQ, RRQ, SAAQ et SQ

Dimension organisationnelle :

- La totalité des M/O rencontrés se sont engagés dans une prestation électronique de services. La grande majorité en sont encore au premier balbutiement avec un stade d'avancement allant de l'étude de faisabilité jusqu'au plan directeur identifiant les potentiels d'affaires, les impacts et les priorités. Certains M/O sont à mettre en place un environnement de développement ou d'expérimentation et les plus avancés ont une première offre de services en place. Ces derniers incluent entre autres la SAAQ avec la clientèle des mandataires en vérification mécanique dans le cadre du projet « Inforoute SAAQ », le MRQ avec le projet « TP1 Internet » et le SERTIR dans le cadre du projet « Brancher les familles » pour le compte du MRCI.
- Les clientèles visées par les PES protégées des M/O couvrent l'ensemble des entités avec lesquelles le gouvernement du Québec transige actuellement. À ce titre on retrouve les individus, les mandataires, les partenaires, les entreprises et organisations privées, les municipalités, les M/O fédéraux, les employés des M/O québécois et les M/O du gouvernement du Québec.
- Dans le cadre des PES protégées et des activités normales des M/O, de multiples échanges d'informations numériques se font actuellement entre les M/O. Certains échanges impliquant des informations numériques personnelles sont réalisés sous l'approbation de la CAI. De plus, la nature et le contenu de ces échanges sont très diversifiés. À la lumière des informations recueillies, tous les M/O ont actuellement des relations d'affaires avec un ou plusieurs M/O impliquant un ou plusieurs types d'échanges d'informations numériques.
- Au niveau de la protection des informations numériques, plus de la moitié des M/O consultés ont effectué un exercice de catégorisation de l'information numérique utilisée ou échangée dans le cadre des PES ou dans le cadre de leurs activités normales. Les méthodes de catégorisation de l'information numérique sont toutefois diverses et la nomenclature utilisée pour désigner le niveau de sensibilité de l'information est variée.
- En ce qui concerne la connaissance des M/O des vulnérabilités inhérentes à leurs informations numériques, les résultats de la cueillette démontrent que la majorité des M/O consultés ont effectué une analyse de vulnérabilités soit pour les PES envisagées ou en cours, soit dans le cadre des activités normales de ces derniers.
- La presque totalité des M/O consultés ont élaboré des politiques, directives, normes et pratiques, guides et procédures en matière de sécurité et ont procédé à l'identification d'un responsable de la sécurité de l'information numérique. Cependant, la moitié des M/O consultés indiquent que le cadre de gestion de la sécurité actuel n'est pas ou est partiellement adapté à la PES.
- Au niveau de la sécurité reliée au personnel, près de la moitié seulement des M/O consultés ont développé jusqu'à présent des plans de sensibilisation et de formation à la sécurité.
- La presque totalité des M/O consultés ont mis en place des mécanismes organisationnels garantissant la sécurité des opérations et la sécurité physique et du milieu. On note cependant une exception, soit la mise en place d'un plan de relève et de continuité. Le quart des M/O consultés n'ont pas encore réalisé cette activité.
- Dans plusieurs M/O, la protection des renseignements personnels, la sécurité et la gestion documentaire sont travaillées de pair.

Les résultats des cueillettes auprès des M/O mettent en évidence un certain nombre de vulnérabilités organisationnelles actuelles :

- Information numérique non-catégorisée dans plusieurs M/O;
- Absence de registre d'autorités de sécurité dans certains M/O;

- Absence d'un plan global de sécurité dans quelques M/O;
- Absence de mécanismes de contrôle et de suivi ainsi que processus d'audit dans un certain nombre de M/O ;
- Enquêtes de sécurité non-effectuées dans la majorité des M/O ;
- Habilitation sécuritaire (ex: processus d'accréditation) non-effectuée dans la majorité des M/O ;
- Manque de sensibilisation/formation dans certains M/O ;
- Aucun plan de relève et de continuité dans quelques M/O.

De même, un certain nombre d'enjeux et d'impacts organisationnels ont été mis en évidence par ces cueillettes :

ENJEUX ET IMPACTS ORGANISATIONNELS

Enjeux	Impacts
➢ Adhésion des utilisateurs ➢ Confiance des utilisateurs ➢ Support des utilisateurs ➢ Facilité d'utilisation des services ➢ Confidentialité des informations numériques ➢ Habilitation des employés ➢ Financement ➢ Gestion des risques en sécurité	➢ Adaptation/élaboration du cadre de gestion de la sécurité (incluant normes, pratiques, mécanismes de contrôle) ➢ Adaptation/élaboration des politiques et directives internes (incluant orientation et principes) ➢ Adaptation/élaboration des processus et guides d'opérations ➢ Formation et sensibilisation du personnel ➢ Adaptation du service à la clientèle ➢ Intégration de la PES ➢ Gestion du changement ➢ Élaboration du plan de sécurité et du plan de communication ➢ Relations de travail ➢ Adaptation/élaboration des processus d'affaires ➢ Nouveaux rôles et/ou responsabilités en sécurité ➢ Adhésion de la haute direction

Les informations recueillies ont permis d'observer que la majorité des M/O consultés ont une bonne couverture des différents domaines de sécurité associés à la dimension organisationnelle. Cependant, on remarque que les M/O doivent adapter leur cadre de gestion de la sécurité à plusieurs niveaux afin de s'assurer que des mesures adéquates sont prises afin de garantir, au niveau approprié, la protection des informations numériques dans le cadre des PES. Plus spécifiquement, des travaux sont nécessaires au niveau de la catégorisation de l'information numérique, du plan global de sécurité et du plan de formation et de sensibilisation. De plus, il est important de souligner qu'il y a un manque de personnel qualifié au niveau de la sécurité.

Dimension technologique :

- La presque totalité des M/O consultés indiquent avoir adressé différents aspects de l'architecture de sécurité. Actuellement un peu plus de la moitié d'entre eux travaillent à l'élaboration ou à l'adaptation de leur architecture de sécurité. Les autres M/O indiquent soit que leur architecture de sécurité actuelle est adaptée à la PES, soit que leur nouvelle architecture est complétée et en attente d'approbation.
- La majorité des M/O consultés ont mis en place des mécanismes de sécurité et des solutions technologiques tels que des coupe-feu, des serveurs de cache ou proxy, des outils de détection des virus et des outils de journalisation et de conciliation des journaux. Cependant seulement la moitié de ceux-ci ont mis en place des réseaux virtuels privés, des outils d'analyse de vulnérabilités, des outils de détection d'intrusions et des mécanismes garantissant la haute disponibilité.
- Au niveau des infrastructures communes, plus de la moitié des M/O consultés dans une première cueillette indiquent leur intention d'utiliser un ou plusieurs services offerts par le gouvernement lorsque qu'ils seront disponibles et qu'il sera avantageux de le faire. Les services identifiés par les M/O incluent ceux offert par une ICP (incluant les services du RDPRM dans le cadre du projet Inforoute SAAQ), le serveur de paiement et les mécanismes de gestion documentaire. Une seconde cueillette met en évidence un certain nombre d'autres mécanismes recherchés par les M/O qui peuvent faire l'objet d'infrastructures communes : outils ou services de répertoire, outils d'ouverture de session simplifiée, outils ou services d'authentification, outils ou services de chiffrement, outils ou service de contrôle d'intégrité et outils facilitant la gestion du consentement.

Les résultats de cette cueillette auprès des M/O mettent en évidence un certain nombre de vulnérabilités technologiques actuelles :

- Aucun chiffrement du trafic à l'aide de la technologie RPV dans certains MO ;
- Absence d'outils d'analyse de vulnérabilité dans la moitié des M/O ;
- Absence d'outils ou services de détection des intrusions dans près de la moitié des M/O ;
- Absence d'outils ou services de journalisation et conciliation des journaux dans certains M/O ;
- Absence d'outils ou services de surveillance évolués (outre la détection des virus) ;
- Absence d'outils ou services de garantie de haute disponibilité.

De plus, plusieurs enjeux et impacts technologiques relatifs à la sécurité de l'information numérique pour une PES protégée ont été recueillis :

ENJEUX ET IMPACTS TECHNOLOGIQUES

Enjeux	Impacts
➢ Utilisation d'infrastructures communes ➢ Gestion de l'habilitation ➢ Gestion unique des identifiants au niveau gouvernemental ➢ Arrimage des technologies entre les M/O ou avec d'autres organisations ➢ Assurance des critères de DICAI ➢ Évolution rapide des technologies	➢ Adaptation/élaboration du cadre de développement et d'acquisition ➢ Ajout de nouvelles fonctions de sécurité ➢ Mise à jour des technologies et ajout de nouvelles technologies ➢ Adaptation/élaboration de l'architecture technologique et de sécurité

Du côté technologique, on remarque que les M/O sont relativement bien équipés afin de répondre aux exigences de sécurité de leurs activités normales. Cependant, plusieurs considérations au niveau de la détection, de la prévention, de la correction et des moyens d'assurance de la sécurité permettent d'établir qu'il existe des besoins additionnels pour une PES protégée. Ces derniers incluent notamment des outils adéquats pour gérer les autorisations d'accès aux données (par exemple lorsqu'elles migrent vers des entrepôts de données et ailleurs par la suite), des outils et services d'analyse de vulnérabilité, de détection des intrusions et de surveillance (réseau, serveurs et données), de conciliation des journaux et de haute disponibilité. De plus, considérant l'évolution technologique très rapide, il est impératif de s'assurer que la révision des technologies devient une activité récurrente.

1.2.3.7 Infrastructures centrales

Cette section présente un résumé de l'état de situation des infrastructures centrales du gouvernement du Québec, soit l'infrastructure du serveur de télécommunication à la DGT et l'infrastructure du serveur informatique gouvernemental à la DGSIG.

Serveur de télécommunication

Le réseau intégré de communications informatiques et bureautiques (RICIB) est un réseau porteur à capacité étendue qui constitue l'ossature de base de l'inforoute gouvernementale. Il est géré par la Direction générale des télécommunications du Secrétariat du Conseil du trésor.

Le RICIB fournit des services d'accès aux banques d'information, de maillage des réseaux locaux, d'accès à un ensemble de services spécialisés de l'inforoute gouvernementale, de communication entre les réseaux des ministères et les réseaux publics et de distribution d'informations de gestion de réseau.

Considérant la demande mettant de plus en plus à l'épreuve les capacités du RICIB et la fin du contrat en cours, le Secrétariat du Conseil du trésor procédait en janvier 2001 au lancement d'un appel d'offres en vue de sélectionner un fournisseur pour la réalisation d'un réseau de plus grande capacité, le Réseau de télécommunication multimédia de l'administration publique québécoise (RETEM). Le RETEM vise à

assurer la convergence des services réseaux, des services Internet et intranet et des services de téléphonie aux M/O.

Étant l'épine dorsale des échanges électroniques au gouvernement du Québec, le RETEM devra être hautement disponible et sécurisé. Dans ce contexte, les lacunes inhérentes à la sécurité du RETEM peuvent constituer des vulnérabilités importantes pour tout l'appareil gouvernemental. Le RETEM devra donc compter sur tous les mécanismes organisationnels et technologiques permettant de garantir la sécurisation des infrastructures technologiques et des informations numériques qui transitent sur le réseau, et ce, dans le respect du cadre juridique en place. Selon les informations disponibles sur le RICIB, il apparaît clairement qu'un certain nombre d'améliorations en matière de sécurité devront être prises en considération pour le RETEM. Mentionnons notamment des améliorations au niveau des éléments suivants[20] :

- **Dimension organisationnelle**

  - Rôles et responsabilités de personnel chargé de la sécurité;
  - Politiques, normes et directives de sécurité spécifiques à la sécurisation du réseau;
  - Guides et procédures de sécurité;
  - Évaluation de vulnérabilités;
  - Plan d'urgence, de relève et de continuité;
  - Mesures d'urgences;
  - Contrôle de l'accès physique;
  - Accès aux serveurs et équipements;
  - Audits;
  - Gestion des changements.

- **Dimension technologique**

  - Coupe-feu (passerelles de sécurité);
  - Systèmes d'exploitation sécurisés;
  - Accès à distance chiffré (RPV; SSH; SSL; ICP);
  - Redondance physique et des fournisseurs de services;
  - Outils d'administration des logiciels et équipements réseau;
  - Analyseur de vulnérabilités sur le réseau et sur les serveurs;
  - Moniteur de contenu actif;
  - Outils de surveillance réseau;
  - Sondes de détection;
  - Détection des tentatives d'intrusions sur le réseau et sur les serveurs associés;
  - Détection de virus sur le réseau et sur la transmission de courrier.

[20] Certains de ces éléments sont déjà en place mais nécessitent des améliorations. D'autres ne sont pas en place. Pour des raisons de sécurité, aucun détail supplémentaire ne sera donné ici.

Serveur informatique gouvernemental

La Direction générale des services informatiques gouvernementaux (DGSIG) a pour mission de fournir aux ministères et organismes qui les requièrent des services informatiques sur diverses plates-formes. Les créneaux qu'elle exploite sont le traitement sur ordinateur, l'accès et la connexité, les conseils en systématisation et en informatisation, des services transactionnels d'information et de repérage (SERTIR) et un centre d'expertise en entrepôts de données (CEED).

Les applications gouvernementales ainsi que les applications clientes des M/O hébergés sur ordinateurs centraux à la DGSIG bénéficient de deux systèmes de sécurité, soit ACF2 ou encore TSS. Ces deux systèmes de sécurité sont au choix des M/O utilisateurs. Une étude de positionnement récente démontre qu'il n'y a pas de bénéfices substantiels à rationaliser sur un seul système.

La DGSIG est responsable de l'installation, de la paramétrisation et de la sécurisation initiale des environnements des M/O. À cet effet, des normes, des pratiques, des guides, etc. sont en place afin de s'assurer notamment des rôles et des responsabilités des intervenants impliqués, du niveau de disponibilité, du type de relève, etc. en fonction des besoins des M/O.

Pour sa part, chaque M/O utilisateur est responsable de la sécurité de ses applications ainsi que de la gestion des identifiants et des profils des utilisateurs. Cette décentralisation de la gestion de la sécurité aux M/O favorise une souplesse d'adaptation aux façons de faire de ceux-ci et minimise les délais reliés à la gestion des accès. Cependant, il n'existe pas de guide ou de référence gouvernementale afin d'assister les M/O dans cette tâche et ainsi uniformiser les pratiques.

Une étude est en cours afin de positionner l'utilisation de USS (services IP de type Unix) sur la plate-forme centrale et de déterminer l'utilisation précise de cette solution par les M/O en fonction des besoins de ces derniers. La DGSIG étudie également plusieurs modes d'arrimage des services d'arrière plan offerts par les plate-formes centrales à des solutions de type Web. On retrouve parmi les solutions envisagées des technologies de queue de messages, de maquillage Web, d'émulation 3270, de pseudo online et même l'utilisation d'un serveur d'application Web s'exécutant sur ordinateurs centraux.

La DGSIG est donc dans un processus d'adaptation de ses services en fonction des nouveaux besoins exprimés par sa clientèle dans le cadre d'une PES protégée.

Dimension juridique :

Tout comme dans le cas des M/O, la DGSIG est confrontée à des lois et règlements qui ne sont pas, dans plusieurs cas, adaptés à un contexte de PES protégée. Il existe certaines zones où des ajustements sont nécessaires. Par exemple, l'hébergement des données à l'extérieur des M/O sur des plate-formes exploitées par des intervenants externes engendre des problématiques, par exemple au niveau des responsabilités et de l'imputabilité des employés de ces intervenants. Des avis juridiques et des ajustements seront probablement requis. Une révision des contrats entre la DGSIG et les M/O est également à prévoir.

Dimension organisationnelle :

Les informations recueillies ont permis d'observer que la DGSIG couvre relativement bien les différents domaines de sécurité associés à la dimension organisationnelle. Cependant, la DGSIG devra probablement

adapter son cadre de gestion de la sécurité afin de s'assurer que des mesures adéquates sont prises afin de garantir, au niveau approprié, la protection des informations numériques dans le cadre des PES. Plus spécifiquement, des travaux sont nécessaires pour supporter les nouvelles solutions d'arrimage des services d'arrière plan offerts par des plate-formes centrales à des solutions de type Web qui seront utilisées dans le cadre des PES protégées des M/O. Des adaptations sont également à prévoir lorsque des outils et des services communs, partagés ou réutilisables seront intégrés aux services de la DGSIG (ex. : ICP, répertoire, etc.).

Dimension technologique :

Les nouvelles solutions d'arrimage des services d'arrière plan offerts par les plate-formes centrales devront tenir compte des besoins de persistance des sessions, de reconnaissance d'identifiants multiples lors d'une transaction, de journalisation de bout en bout, etc. Les technologies retenues devront donc, lorsque nécessaire, supporter ces fonctionnalités selon des normes et standards ouverts et reconnus afin de favoriser l'utilisation potentielle d'outils et de services communs, partagés ou réutilisables (ex : ICP, répertoire, etc.)

1.3 Exigences architecturales en matière de sécurité

Pour supporter les grandes orientations de l'État, l'architecture d'entreprise gouvernementale (AEG) a élaboré des stratégies d'affaires et des exigences architecturales. Les tableaux suivants mettent en évidence celles qui ont un rapport direct avec la sécurité de l'information numérique (*texte en italique*). Ce rappel des stratégies d'affaires et des exigences architecturales est enrichi de nouvelles stratégies d'affaires ou d'exigences architecturales spécifiques en matière de sécurité de l'information numérique (*texte en italique et souligné*). [21]

Les stratégies d'affaires et les exigences architecturales ci-dessous sont tirées de la version 3,0 du 6 décembre 2000 de l'AEG[22], qui précisons-le, n'a pas encore fait l'objet d'une approbation. Rappelons que l'AEG vise à supporter les trois grands axes d'intervention de la Loi sur l'administration publique soient :

- La qualité des services ;
- La performance de l'Administration publique ;
- Le développement de la société québécoise.

[21] Pour une vision complète des stratégies d'affaires et des exigences architecturales élaborées dans l'AEG, incluant celles élaborées dans le cadre de l'AGSIN, on consultera l'annexe F.

[22] Notons que certaines stratégies d'affaires de l'AEG ne sont pas directement appuyées par des exigences architecturales en matière de sécurité; ces stratégies d'affaires n'apparaissent donc pas ici mais uniquement à l'annexe F.

STRATÉGIES D'AFFAIRES ET EXIGENCES ARCHITECTURALES EN MATIÈRE DE SÉCURITÉ

QUALITÉ DE LA PRESTATION DE SERVICES AUX INDIVIDUS	
Stratégies d'affaires	**Exigences architecturales en matière de sécurité**
Disponibilité et accessibilité : ▪ Disponibilité pratiquement continue du service ▪ Soutien 24 heures sur 24, 7 jours / semaine lorsque requis ▪ Accessibilité à l'ensemble du territoire sous réserve de la disponibilité des infrastructures appropriées	▪ *La prestation électronique de services doit être supportée par des mécanismes qui permettent d'assurer la sécurité de l'information numérique en tout temps et sur l'ensemble du territoire.*
Simplicité et convivialité : ▪ Niveau de convivialité accrue pour l'utilisateur ▪ Prestation dans la langue de l'utilisateur ▪ Personnalisation du service selon les besoins et le contexte de l'utilisateur ▪ Soutien à l'utilisateur adapté à ses spécificités	▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.*
Efficacité : ▪ Rapidité de réponse aux requêtes de l'utilisateur ▪ Diligence de livraison des produits et services demandés ▪ Fiabilité et pertinence du résultat obtenu	▪ *Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place doivent permettre d'assurer l'intégrité et l'irrévocabilité lorsque nécessaire.*
Équité : ▪ Niveau de service acceptable pour tout utilisateur, peu importe l'endroit d'où est requis le service	▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.*
Sécurité : ▪ *Sécurité garantie (adéquate) des transactions (communications) électroniques* ▪ *Protection adéquate des renseignements personnels*	▪ *L'environnement de soutien à la prestation électronique de services est sécurisé en fonction du cadre légal et réglementaire en vigueur au Québec, et de manière à inspirer confiance à l'utilisateur.*

STRATÉGIES D'AFFAIRES ET EXIGENCES ARCHITECTURALES EN MATIÈRE DE SÉCURITÉ

PERFORMANCE DE L'ADMINISTRATION PUBLIQUE	
Stratégies d'affaires	**Exigences architecturales en matière de sécurité**
Efficacité des employés : ▪ Accroissement de l'efficacité dans un contexte de réorganisation du travail	▪ *Les mécanismes de sécurité doivent permettre d'assurer la protection des renseignements personnels durant tout le cycle de vie de l'information.*
Compétitivité du gouvernement : ▪ Réduction des coûts globaux de fonctionnement ▪ Amélioration de l'expertise dans les nouvelles technologies ▪ Projection d'une image d'efficacité et de compétence	▪ En tant que levier de développement, la prestation électronique de services permet notamment de rendre disponible : ▫ *Des mécanismes reconnus et harmonisés en matière de sécurité de l'information numérique.*
Réduction des coûts d'opération : ▪ Coûts globaux de fonctionnement ▪ Économie d'échelle ▪ Coût de prestation des services ▪ Coût de gestion des programmes	▪ *Les mécanismes de sécurité doivent présenter un rapport risques/coûts acceptable.*
Contribution du secteur privé : ▪ Partenariats avec l'entreprise privée	▪ *L'arrimage entre l'Administration publique et l'entreprise privée doit se faire dans un environnement sécurisé afin de protéger les renseignements personnels et la vie privée.*
Partage entre les organisations : ▪ Intégration de services multi-organisations ▪ Économies d'échelle ▪ Services communs	▪ *Les solutions envisagées pour simplifier et intégrer les mécanismes de communication électronique doivent permettre d'assurer la sécurité de l'information numérique.*

STRATÉGIES D'AFFAIRES ET EXIGENCES ARCHITECTURALES EN MATIÈRE DE SÉCURITÉ

LEVIER DE DÉVELOPPEMENT SOCIAL, CULTUREL ET ÉCONOMIQUE	
Stratégies d'affaires	**Exigences architecturales en matière de sécurité**
Adoption des nouvelles technologies par les individus : ▪ Utilisation accrue des NTIC ▪ Échanges et transactions avec le gouvernement	▪ *L'environnement de soutien à la prestation électronique de services est sécurisé de manière à respecter le cadre légal et réglementaire en vigueur au Québec, et inspirer confiance à l'utilisateur.* ▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.*
Adoption des nouvelles technologies par les entreprises : ▪ Utilisation et développement de l'autoroute de l'information ▪ Commerce électronique	▪ *L'environnement de soutien à la prestation électronique de services est sécurisé de manière à respecter le cadre légal et réglementaire en vigueur au Québec, et inspirer confiance à l'utilisateur.* ▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.*
Promotion du Québec : ▪ Localement et à l'étranger ▪ Image de modernité	▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.* ▪ *La prestation électronique de services doit être supportée par des mécanismes qui permettent d'assurer la sécurité de l'information numérique en tout temps et sur l'ensemble du territoire.*
Rehaussement du potentiel d'exportation de l'industrie des TIC : ▪ Normes internationales ▪ Produits et services d'avant-garde	▪ *L'architecture de la sécurité de la prestation électronique des services est fondée sur les normes les plus ouvertes de l'industrie en matière de sécurité afin de maximiser son évolutivité.*

1.4 Principes en matière de sécurité de l'information numérique

Les principes visent à encadrer de manière spécifique la protection de l'information numérique dans la perspective d'une utilisation des technologies de l'information et des communications au service des grandes orientations de l'État.

Le point 1.4.1 présente les principes et les responsabilités de la Directive. Le point 1.4.2 propose des principes complémentaires dans le cadre du projet AGSIN. Rappelons que la Directive et ses principes ne couvrent que l'information numérique tout comme les principes proposés par le projet AGSIN.

1.4.1 La directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration publique

Les principes présentés dans cette section sont ceux de la Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale, en vigueur depuis février 2000.

1.4.1.1 Objet de la Directive

Cette directive énonce les principes directeurs en matière de sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale, identifie les intervenants concernés par la gestion de cette sécurité, détermine les responsabilités des ministères et organismes et prévoit l'instauration des mécanismes appropriés de coordination et de collaboration en vue d'assurer la disponibilité, l'intégrité, la confidentialité de l'information numérique, l'authentification des utilisateurs et l'irrévocabilité des documents qu'ils rédigent ou des actions qu'ils posent.

1.4.1.2 Champ d'application

Cette directive s'applique aux ministères et aux organismes dont le budget de fonctionnement est voté, en totalité ou en partie, par l'Assemblée nationale ou dont le personnel est nommé et rémunéré suivant la Loi sur la fonction publique (chapitre F-3.1.1).

Cette directive s'applique également à tout autre organisme public qui adhère à une infrastructure commune du gouvernement du Québec.

1.4.1.3 Principes directeurs

- La sécurité contribue à la réalisation de la mission de l'État en protégeant sa renommée et la confiance des individus à l'égard des services publics. Elle prend tout son sens dans la poursuite des finalités de l'organisation dans le respect des obligations légales et administratives.

  Les ministères et organismes, qui sont les premiers responsables d'assurer la sécurité de l'information numérique qu'ils détiennent ou utilisent ainsi que celle des échanges électroniques, doivent mettre en oeuvre un ensemble de mesures destinées à gérer les risques et leurs impacts à l'égard de :

  a) la « **disponibilité** », laquelle est la propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée ;
  b) l'« **intégrité** », laquelle est la propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation ;
  c) la « **confidentialité »**, laquelle est la propriété d'une information de n'être accessible qu'aux personnes autorisées ;
  d) l'« **authentification** », laquelle est un acte permettant d'établir la validité de l'identité d'une personne ou d'un dispositif ;
  e) l'« **irrévocabilité** », laquelle est la propriété d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.

- Le sous-ministre ou le dirigeant d'organisme doit assurer la gestion de la sécurité conformément aux principes suivants :

    a) **vision commune** : l'atteinte d'un niveau de sécurité adéquat nécessite l'adhésion à une vision et une compréhension communes de la sécurité tant au sein des ministères et organismes que dans l'Administration gouvernementale ;
    b) **cohérence** : la sécurité repose sur une approche globale et intégrée qui tient compte des aspects humains, organisationnels, physiques, techniques et juridiques et demande la mise en place d'un ensemble de mesures coordonnées de prévention, de détection, de correction et de sanction ;
    c) **responsabilité et imputabilité** : l'efficacité de la sécurité exige l'attribution claire de responsabilités à tous les niveaux de l'organisation et la mise en place de mécanismes de coordination et de contrôle permettant une reddition de comptes adéquate ;
    d) **évolution** : les pratiques et solutions techniques retenues en matière de sécurité doivent être réévaluées périodiquement afin de tenir compte des changements organisationnels et technologiques ainsi que de l'évolution des menaces et des risques ;
    e) **universalité** : les pratiques et solutions techniques retenues en matière de sécurité correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.

1.4.2 Les principes généraux et spécifiques complémentaires

Compte tenu de la nature et de la portée de l'architecture d'entreprise gouvernementale en matière d'utilisation des technologies de l'information et des orientations qu'elle supporte, d'autres principes en matière de sécurité de l'information numérique sont proposés ci-dessous. Les principes complémentaires couvrent la sécurité de l'information numérique dans toutes les étapes de son cycle de vie et dans tous les types d'échange et non uniquement la PES.

Ces derniers sont proposés en complémentarité à ceux existants dans la Directive afin de supporter les grandes orientations gouvernementales.

1.4.2.1 Principes généraux

- Les ministères et organismes, qui sont les premiers responsables d'assurer la sécurité de l'information numérique, doivent dans l'utilisation des technologies de l'information et des communications mettre en place un environnement humain, organisationnel, physique, technique et juridique qui favorise la sécurité de l'information numérique durant tout le cycle de vie de l'information, dans le respect des normes légales de protection des renseignements personnels et confidentiels, de la propriété intellectuelle et des droits d'auteurs et dans le plus grand respect de la vie privée des personnes concernées.
- Les ministères et organismes doivent mettre en place des solutions en matière de sécurité de l'information numérique dans le respect du cadre légal et réglementaire en vigueur au Québec, et de manière à inspirer confiance aux citoyens et à respecter la mission de l'État.

1.4.2.2 Principes spécifiques

- Le ministère ou l'organisme ne recueille, n'enregistre et ne conserve que les renseignements personnels nécessaires à l'exercice de ses fonctions ou la mise en œuvre d'un programme dont il a la gestion. Il ne les rend accessibles qu'aux personnes autorisées (employés de l'État ou autres) lorsque cela est nécessaire à l'exercice de leurs fonctions.
- Un ministère ou organisme qui recueille des renseignements auprès d'un individu ou d'un représentant de l'entreprise l'informe de l'usage qui sera fait des renseignements personnels, confidentiels ou stratégiques qu'il fournit et de tout autre usage qui pourrait en être fait.
- Le ministère ou l'organisme obtient un consentement explicite, libre, éclairé, spécifique et limité dans le temps auprès de l'individu concerné ou du représentant de l'entreprise concernée pour recueillir, utiliser, modifier, communiquer et détruire des renseignements personnels, confidentiels ou stratégiques. Dans le cas ou la loi autorise la collecte, l'utilisation ou la communication de ces renseignements sans le consentement des personnes concernées, le ministère ou l'organisme prend les mesures nécessaires pour les informer de l'usage projeté des renseignements dans sa propre organisation ou ailleurs.
- Le ministère ou l'organisme facilite à l'individu et au représentant de l'entreprise l'exercice du droit d'accéder aux renseignements numériques le concernant et de demander à rectifier les anomalies s'il y lieu, en temps voulu et selon les dispositions législatives en vigueur.
- Le ministère ou l'organisme garantit la localisation de l'information numérique, de manière sécurisée, durant tout son cycle de vie.
- Le ministère ou l'organisme met en place des mécanismes afin d'assurer, en tout temps, la sécurité de l'information stratégique[23] de l'État et la protection des renseignements personnels et confidentiels tout au long de son cycle de vie.
- Le ministère ou l'organisme catégorise l'information numérique afin de déterminer sa valeur et d'appliquer les mesures de sécurité adéquates en fonction d'une gestion des risques et des impacts en regard des critères de DICAI.
- Le ministère ou l'organisme doit assurer la compatibilité et l'interopérabilité des supports et des technologies afin de supporter, en tout temps, la sécurité de l'information numérique durant son cycle de vie.

[23] Cette définition est tirée des travaux du passage de l'an 2000 : l'information stratégique est celle qui est utilisée ou requise par les systèmes stratégiques (les systèmes qui sont de première importance pour la réalisation de la mission du ministère ou de l'organisme) et par les activités essentielles à l'accomplissement de la mission du gouvernement du Québec (un service ou une fonction exécutés par un ministère ou un organisme ayant une incidence sur la santé et la sécurité du public, et la stabilité économique de l'État, dont la perte ou l'interruption, même pendant une courte période, est considérée susceptible d'occasionner un risque inacceptable).

2. LE MODÈLE GÉNÉRAL DE L'AGSIN (PERSPECTIVE LOGIQUE)

Élément essentiel de la PES, l'AGSIN est abordée sous l'angle de l'information et des applications, et non pas uniquement sous l'angle de la technologie, et tient compte de la nécessité d'assurer l'identification des parties notamment pour la protection des renseignements personnels. D'autre part, la prise en considération des diverses étapes du cycle de vie de l'information garantit que l'ensemble des besoins et préoccupations en matière de sécurité sera pris en compte.

L'AGSIN touche à tous les volets architecturaux (affaires, information, application et infrastructure) et fait ressortir l'ensemble des impacts inhérents à la sécurité au sein des M/O et des organisations sous la gouvernance de l'État, que ce soit au niveau de la dimension juridique, organisationnelle, humaine ou technologique. L'AGSIN se veut être un guide pour ces derniers en rassemblant et en précisant les composantes de sécurité qui s'appliquent dans les autres volets architecturaux et en présentant ces composantes dans un ensemble cohérent, simple et à haut niveau afin d'obtenir une image complète de la sécurité de l'information numérique. Elle permet ainsi un encadrement des travaux d'architectures de sécurité de l'information numérique (ASIN) des M/O et organisations sous la gouvernance de l'État.

Enfin, l'AGSIN assure, au niveau gouvernemental, la cohérence face aux diverses clientèles avec lesquelles le gouvernement du Québec peut être amené à transiger et fait ressortir les composantes ayant un potentiel de mise en commun, de partage ou de réutilisation.

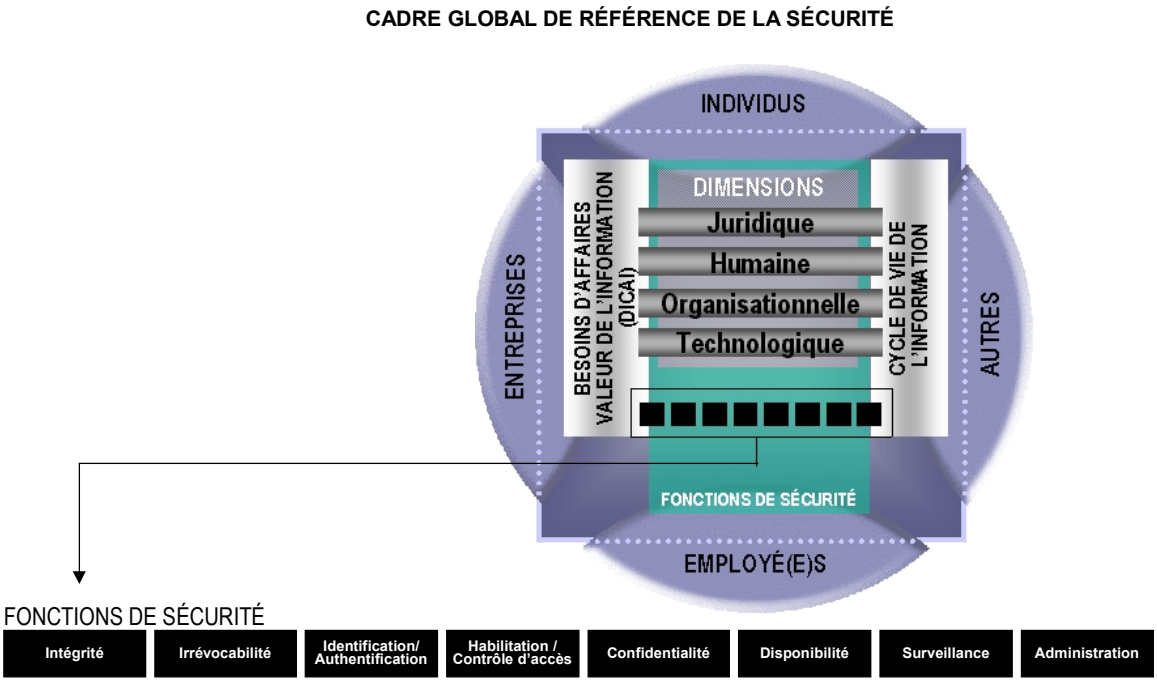
2.1 Cadre global de référence

Se doter d'un cadre global de référence permet de manière simple et efficace de visualiser les éléments dominants à considérer dans la sécurité de l'information numérique. De plus, ceci permet la mise en contexte des différents éléments du concept d'espace sécurisé introduit dans la première version de l'architecture d'entreprise gouvernementale.

Ainsi le cadre global de référence met en perspective :

- les besoins d'affaires;
- le cycle de vie de l'information;
- les clientèles visées (les individus (citoyens), les entreprises, les employé(e)s de l'état et les autres clientèles (ex : fournisseurs, mandataires, autres gouvernements, etc.) adressées par l'AGSIN;
- les dimensions (juridique, humaine, organisationnel et technologique) à considérer pour créer un climat de confiance au sein des M/O, des organisations sous la gouvernance de l'État et des clientèles concernées par les échanges électroniques sécuritaires, le tout en fonction des besoins d'affaires, du cycle de vie de l'information et de la valeur de l'information ;
- les fonctions de sécurité, supportées par un ensemble de mécanismes de sécurité et de solutions technologiques, permettant la protection de l'information numérique et l'établissement des échanges électroniques protégés.

La figure suivante illustre le cadre global de référence de la sécurité :



2.2 Les clientèles visées

Dans sa phase initiale de conception, l'AEG s'est limitée à la définition de la prestation électronique de services aux individus et aux entreprises. L'AGSIN quant à elle doit couvrir plus globalement l'échange de l'information numérique. Ceci inclut non seulement les échanges avec les individus et les entreprises, mais aussi avec les autres clientèles ainsi que les relations avec les systèmes existants, les échanges avec les fournisseurs du gouvernement, les mandataires, les partenaires, les autres gouvernements ainsi que ceux à l'interne entre les organisations gouvernementales.

C'est ainsi que les domaines de confiance[24] qui seront adoptés doivent impérativement prendre en considération l'ensemble des communications électroniques que le gouvernement du Québec aura avec l'ensemble de ses clientèles.

Plus spécifiquement, l'AGSIN distingue quatre (4) types de clientèles, chacune présentant des caractéristiques particulières, à savoir:

- Les individus (citoyens), lesquels sont directement concernés par les problématiques de respect de la vie privée et de protection des renseignements personnels;
- Les associations et les entreprises, que ce soit pour s'acquitter de leurs obligations légales ou fiscales ou pour offrir des biens et services dans le cadre des marchés publics. Les fournisseurs sont également une clientèle faisant des échanges avec le gouvernement;

[24] On consultera la section 2.7 pour plus d'informations sur le concept de domaines de confiance.

- Les employés de l'état, qui sont des utilisateurs aux caractéristiques homogènes et pour lesquels la mise en place des mesures de sécurité est entièrement sous le contrôle du gouvernement du Québec;
- Les mandataires du gouvernement du Québec et de ses clients qui, à des degrés divers, sont intégrés aux processus d'affaires des M/O concernés. Ceux-ci font le lien entre l'individu ou l'entreprise et le gouvernement du Québec.

2.3 Valeur de l'information (DICAI) et le cycle de vie de l'information

Les besoins d'affaires (exigences nées d'une série de processus, ayant chacun une finalité clairement définie, impliquant plus d'une organisation, réalisés par échange d'informations et tendant à l'accomplissement d'un objectif accepté par accord mutuel pour une certaine période de temps) doivent être clairement exprimés et définis dès le début.

Les critères de DICAI (disponibilité – intégrité – confidentialité – authentification – irrévocabilité), présentés dans la « Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale »[25], sont des assises importantes de la sécurité dans les affaires électroniques. Ils permettent d'évaluer et de gérer adéquatement les risques liés à la disponibilité, l'intégrité et la confidentialité des informations numériques ainsi qu'à l'authentification des intervenants et à l'irrévocabilité des actes juridiques ou administratifs posés.

Il importe de mentionner que l'étendue des menaces et des risques liés aux différentes catégories d'informations numériques ou d'échanges électroniques sera un facteur déterminant dans le choix des mécanismes de sécurité et solutions technologiques retenus. Ici, les informations à protéger sont catégorisées selon leur valeur et font l'objet d'une évaluation sur chacun des attributs (critères) de DICAI. On y précise également leur contexte d'utilisation, c'est-à-dire si l'information se véhicule sur un poste autonome ou mobile, un réseau fermé ou un réseau ouvert. Pour une même information, les mesures de sécurité peuvent effectivement varier selon le contexte.

La mise en œuvre de l'AGSIN implique que dans le cadre d'un projet d'affaires précis, les sources de risques et menaces sont telles qu'il faille utiliser une solution de sécurité de niveau adéquat pour assurer la fiabilité des informations numériques ou des transactions électroniques afin de les faire accepter au besoin, en preuve devant les tribunaux.

Après avoir reconnu l'importance des critères de DICAI de la Directive sur la sécurité, il faut aussi reconnaître l'importance du maintien de ces critères dans chacune des étapes du cycle de vie de l'information (définition, création, enregistrement[26], traitement, diffusion, conservation et destruction de l'information).

C'est aussi l'une des prémisses sur lesquelles repose la loi concernant le cadre juridique des technologies de l'information qui énonce que la fiabilité d'un document repose sur son intégrité, quel qu'en soit le support tout au long de son cycle de vie. Le passage d'un document (ou d'une information) entre les différentes étapes de son cycle de vie devient donc une considération de première importance pour le maintien de la validité juridique du document.

[25] On se référera à la *Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'Administration gouvernementale* pour plus de détails sur le site du SCT.
[26] L'entregistrement inclut la réception de l'information venant de l'externe ou de la clientèle.

La responsabilité des officiers ou administrateurs ne fait donc aucun doute en regard de l'évaluation et du maintien du niveau de sécurité tout au long du cycle de vie de l'information.

2.4 Les dimensions de la sécurité

La pratique veut qu'on subdivise les éléments à considérer dans la sécurisation des infrastructures technologiques, des applications et des informations numériques en différents aspects de la sécurité. Cette approche est utilisée entre autres dans la norme ISO/IEC 17799[27], la « norme de sécurité technique dans le domaine de la technologie de l'information » de la Gendarmerie Royale du Canada et l'architecture de sécurité du gouvernement de l'état de la Caroline du Nord. Le modèle holistique, résumé ici et détaillé dans les sections 2.4.1 à 2.4.4, est un amalgame représentatif des modèles présentés par ces différentes organisations.

Les différentes dimensions de la sécurité et les aspects et points particuliers qu'elles renferment devront être considérés par les divers individus responsables de la sécurité dans les M/O, de même que par les intervenants impliqués dans l'élaboration de toute architecture de sécurité de l'information numérique (ASIN).

[27] On consultera l'annexe D pour plus de détails sur cette norme.

DIMENSIONS DE LA SÉCURITÉ

Dimension juridique	Aspects légaux	➢ Lois et règlements nationaux ➢ Lois et règlements provinciaux généraux et spécifiques ➢ Conventions internationales ➢ Contrats et ententes ➢ Avis juridiques
Dimension humaine	Sécurité du personnel	➢ Enquête de sécurité ➢ Habilitation sécuritaire ➢ Sensibilisation à la sécurité ➢ Formation du personnel
	Éthique, pratique professionnelle et imputabilité	➢ Responsabilités de l'organisation ➢ Responsabilités des gestionnaires ➢ Responsabilités du personnel et des usagers
Dimension organisationnelle	Sécurité administrative	➢ Politiques, normes, directives, guides et procédures de sécurité ➢ Rôles et responsabilités du personnel chargé de la sécurité ➢ Catégorisation de l'information ➢ Évaluation de vulnérabilité (menaces/risques) ➢ Registres et dossiers de sécurité ➢ Gestion du consentement ➢ Prévention
	Sécurité physique et du milieu	➢ Installations principales et auxiliaires des ressources informationnelles ➢ Contrôle de l'accès physique ➢ Sécurité du matériel
	Sécurité des opérations	➢ Administration ➢ Contrôle d'accès logique ➢ Surveillance et audit ➢ Utilisation et gestion des supports ➢ Mesure d'urgence, de relève et de continuité
Dimension technologique	Sécurité des logiciels, du matériel, des communications et des informations de sécurité	➢ Fonctions de sécurité : ▪ Intégrité ▪ Irrévocabilité ▪ Identification/Authentification ▪ Habilitation/Contrôle d'accès ▪ Confidentialité ▪ Disponibilité ▪ Surveillance ▪ Administration ➢ Développement des applications ➢ Sélection des applications ou équipements ➢ Installation et paramétrisation des applications ou équipements

2.4.1 Dimension juridique

L'AGSIN a pour but d'assister les intervenants en sécurité dans l'élaboration d'une architecture de sécurité de l'information numérique (ASIN) reposant sur le respect des critères de DICAI de la « Directive sur la sécurité de l'information numérique et des échanges électroniques dans l'administration gouvernementale ». Cependant, la mise en œuvre d'une telle architecture doit aussi rencontrer des critères organisationnels, humains, technologiques et juridiques afin de maintenir le haut niveau de sécurité recherché.

Dans le cadre d'un projet de sécurité, la dimension juridique figure parmi les aspects à articuler à l'intérieur de toute architecture de l'information numérique[28]. Cette dimension n'étant pas autonome par elle-même, elle doit être supportée par les autres dimensions de la sécurité, soit les dimensions humaine, organisationnelle et technologique. C'est aussi une dimension « tentaculaire » en ce sens qu'elle touche tous les éléments conceptuels du cadre de référence. Ainsi, la dimension juridique concerne les relations avec les individus, les entreprises, les employés et les autres clientèles. Elle prend également tout son sens en regard des besoins d'affaires liés à DICAI, elle s'applique dans toutes les étapes du cycle de vie de l'information et elle est supportée par les fonctions de sécurité.

Afin de pouvoir présenter les grandes lignes de la dimension juridique, il convient de présenter les prémisses nécessaires à la compréhension des aspects de cette dimension :

- L'information numérique a été inventoriée, évaluée et catégorisée en regard des critères de DICAI afin de déterminer le niveau de sécurité requis : faible, moyen, élevé;
- Toutes les analyses visant à déterminer, évaluer et reconnaître les risques et les menaces liés à la sécurité des informations ou documents numériques ont été faites de façon à bien cibler les informations numériques nécessitant les protections juridiques soulevées dans cette section;
- Les différentes étapes de vie (définition, création, enregistrement, traitement, diffusion, conservation et destruction de l'information) de chaque information numérique ont été identifiées et sont connues au moment de l'évaluation de la dimension juridique de l'ASIN;
- Un exercice de repérage de l'information numérique à caractère nominatif ou confidentiel a été fait de façon à appliquer à cette information une ASIN qui répond de façon appropriée aux besoins juridiques;
- La dimension est restreinte au contexte juridique applicable au Québec étant donné que la majorité des M/O ont comme mission de rendre des services à la population Québécoise;
- Les intervenants ont impliqué les ressources juridiques de leur M/O, lesquels connaissent de façon plus précise le domaine d'affaires du projet et sont à même de raffiner l'approche juridique de l'ASIN à mettre en place;
- L'ASIN doit considérer l'intégration des dimensions humaine, organisationnelle et technologique pour répondre aux impératifs des aspects juridiques;
- L'ASIN prévoit un processus de révision périodique des procédés, systèmes et autres paramètres de l'architecture de sécurité existante, de façon à maintenir le niveau approprié de sécurité dans le temps.

[28] On consultera les documents *Architecture gouvernementale de la sécurité de l'information numérique – Portrait et besoins gouvernementaux* et *Architecture gouvernementale de la sécurité de l'information numérique – Orientations et principes* pour plus d'informations.

Les sections qui suivent décrivent les différents éléments des dispositions législatives, chartes des droits et libertés, contrats, ententes, conventions et autres considérations d'ordre juridique devant être considérés par les intervenants impliqués dans l'élaboration d'une ASIN.

2.4.1.1 Les dispositions législatives

Afin de bien orienter les intervenants sur ce qu'ils doivent prendre en considération pour respecter le cadre législatif en vigueur, les points suivants sont adressés :

- Loi sur les archives (L.R.Q., ch. A-21.1);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., ch. A-2.1);
- Loi sur l'administration publique (PL 82);
- Loi concernant le cadre juridique des technologies de l'information (PL 161);
- Certaines dispositions pertinentes du Code civil du Québec (C.C.Q.);
- Loi sur la protection des renseignements personnels dans le secteur privé (P-39.1);
- Loi sur la protection des renseignements personnels et les documents électroniques (C-6);
- Loi sur le droit d'auteur (L.R. 1985, ch C-42);
- Lois sur la propriété intellectuelle et les marques de commerce (L.R. 1985 ch. T-13);
- Lois sectorielles.

Les quatre premières lois sont celles qui auront le plus d'impacts sur la réalisation d'une ASIN.

1) Loi sur les archives (L.R.Q., ch. A-21.1)

La Loi sur les archives s'applique aux archives publiques et aux archives privées. Elle s'applique notamment à tout document (soit tout support d'information, y compris les données qu'il renferme, lisible par l'homme ou la machine). Ses dispositions varient selon que les documents sont actifs, semi-actifs ou inactifs.

Pour être conforme aux dispositions de cette loi, les intervenants impliqués dans l'élaboration d'une ASIN, devront, en ce qui a trait aux informations numériques[29] ayant trait au projet, s'assurer notamment :

- De l'existence d'une politique de gestion des documents actifs et semi-actifs de l'organisme public[30]. Si cette politique n'existe pas, il faudra en établir une et la diffuser adéquatement.
- De vérifier l'existence d'un calendrier de conservation et le mettre à jour au besoin; ou
- D'établir un calendrier de conservation déterminant:

[29] On peut penser ici aux clés publiques et à leur certificat, une autorisation, un courriel, un document Word, un fichier de travail, une copie de sécurité, des données dans une table DB2, copie de programme, les données de journalisation, les demandes d'abonnement, les données d'horodatation etc.

[30] Noter qu'il en existe une pour l'ensemble des M/O (voir annexe de la loi), laquelle est approuvée par le Conseil du trésor. Cette politique est coordonnée et mise en œuvre par le Conservateur des Archives nationales du Québec. Les autres organismes publics (tels org. Santé et services sociaux) doivent adopter leur propre politique.

- Les périodes d'utilisation des documents;
- Les supports de conservation des documents;
- Quels documents sont conservés de manière permanente;
- Quels documents pourront être éliminés;

- De prévoir la mise à jour périodique du calendrier de conservation en fonction des nouveaux impératifs liés au projet;
- D'assurer l'obtention des autorisations requises pour la destruction des documents/informations en temps voulu (soit préalablement à la destruction) et prévoir la conservation de ces autorisations pour la période prévue au calendrier.

Quoique l'AGSIN ne traite que de la sécurité de l'information numérique, ces vérifications devront être faites tant pour les informations « papiers » que numériques.

Notons que les dispositions prises en regard de cette loi ne devront pas entrer en conflit avec les dispositions des lois d'accès à l'information qui prévoient notamment la destruction des informations lorsque l'usage qui devait en être fait a été réalisé.

À titre d'exemple :

Dans le cadre d'un projet d'architecture de la sécurité de l'information numérique, cette loi conditionnera notamment : l'archivage des clés publiques et des certificats, la conservation des demandes d'abonnements, les données des audits et les extractions ou rapports qui ont été produits, la conservation des données d'horodatage ou toutes autres données jugées pertinentes en fonction des processus mis en œuvre.

Selon l'importance accordée à chacun des documents faisant partie des processus d'affaires, le calendrier de conservation devra être adapté pour correspondre à la politique de gestion de tels documents selon les prescriptions prévues ou la durée potentielle durant laquelle un tel document pourra être requis pour preuve. Un exercice d'inventaire et d'évaluation devra être planifié.

2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., ch. A-2.1)

Au Québec, la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[31] s'applique aux renseignements sous la gestion d'un ministère ou organisme public. Cette loi impose plusieurs principes de gestion à ces organismes que les intervenants impliqués dans le processus d'élaboration d'une ASIN pourront s'assurer de couvrir en validant les points suivants après avoir bien inventorié les informations numériques touchant au projet :

- Divulguer les fins de la collecte des renseignements demandés :
  - S'assurer de la divulgation de cette information, que cette information soit requise sur un site WEB ou dans un formulaire électronique ou par tout autre moyen;
  - Divulguer également si l'information doit servir à plus d'un organisme ou ministère et bien les identifier;

[31] Cette loi touche la protection des renseignements personnels des individus et non ceux relatifs aux personnes morales.

  - S'assurer de conserver la preuve de la divulgation.
- Obtenir le consentement à la collecte de ces renseignements (voir les sections 2.4.1.4 et 2.4.3.1 pour plus de détails sur le consentement);
- Obtenir l'autorisation à l'utilisation et à la communication des renseignements sauf si cela n'est pas approprié;
  - Essayer de prévoir les utilisations potentielles de l'information et à qui elle sera communiquée et obtenir une autorisation de la personne concernée. Si cet exercice ne peut être fait en début de projet, il faudra prévoir une approche itérative de façon à couvrir les situations au fur et à mesure où elles seront décelées, que ce soit en cours de projet ou durant les opérations courantes[32] ;
- Planifier la gestion des droits d'accès aux renseignements
  - Assurer une gestion par profils (planifier l'ASIN en conséquence mais mettre aussi en place une structure organisationnelle et fonctionnelle adéquate);
  - Prévoir la signature d'une entente par toute personne désirant obtenir un profil sur un système;
  - Planifier les restrictions prévues;
  - Prévoir les conditions de révocation et de suspension des profils;
  - Planifier le qui, le quoi, le comment et le quand (par exemple si période de temps limitée);
  - Tenir un registre des communications de renseignements (prévoir ce qu'il faut dans l'ASIN);
  - Indiquer comment les contraventions seront traitées (implication nécessaire des volets humain, organisationnel et technologique);
- Protéger les renseignements personnels
  - Prévoir des espaces sécurisés pour la conservation des informations (physiques mais aussi par cloisonnement des zones);
  - Prévoir des contrôles de sécurité rigoureux pour les accès non autorisés, l'utilisation, la modification, la reproduction, la destruction, la perte, le vol, la divulgation non autorisés des renseignements personnels;
  - Assurer la sécurité physique des installations;
  - Prévoir le chiffrement des données et des communications;
  - Planifier la protection de l'information durant tout le cycle de vie de ces renseignements personnels;
  - Prévoir une procédure d'intervention en cas d'incident;
  - Planifier des méthodes d'approbation et d'implantation des changements (documentation des modifications et mesures de sécurité préalablement requises);
  - Publiciser les changements.
- Assurer la destruction des renseignements personnels lorsqu'ils ne sont plus requis (limitation à la conservation) :
  - S'assurer d'être cohérent avec les dispositions du calendrier de conservation (lorsque l'objet pour lequel un renseignement cueilli a été accompli, l'organisme public doit le détruire sous réserve des dispositions de la loi sur les Archives);
  - Prévoir les autorisations lorsque requises et assurer la conservation de celles-ci;
  - Prévoir des modes de destruction adéquats et sécuritaires.

[32] Se référer aux points traitant du consentement pour assurer la validité de l'autorisation (sections 2.4.1.4 et 2.4.3.1)

- Donner accès à la personne concernée par un renseignement nominatif :
  - Prévoir des mécanismes d'accès à l'information pour les personnes concernées. Ces mécanismes pourront être informatisés ou non selon la situation;
  - Informer sur la façon dont la consultation peut être faite et les modalités afférentes. Noter que la réglementation actuelle prévoit la gratuité de ce service sauf s'il y a retranscription d'information, auquel cas seuls les frais de retranscription pourront être exigés.
- Donner le droit de contrôle de l'exactitude à la personne concernée par un renseignement nominatif :
  - Prévoir des mécanismes et procédures pour que les personnes concernées puissent valider l'information qui les concerne;
  - Planifier l'assistance humaine lorsque requise;
  - Assurer que les mêmes croisements d'information, compilation, comparaison pourront être répétés au bénéfice de l'individu qui désire consulter, lorsque requis;
- Rectifier les renseignements lorsque demandé par la personne concernée par un renseignement nominatif :
  - Prévoir les mécanismes et modalités de rectification;
  - Assurer la journalisation de la rectification;
  - Assurer la conservation de l'ancienne information (celle erronée) sans que celle-ci ne puisse être utilisée ultérieurement;
  - Assurer la diffusion des informations rectifiées lorsque celles-ci touchent (ou servent) plusieurs organisations.
- Prévoir un processus systématique pour que cette évaluation soit faite à chaque fois que de nouvelles informations seront ajoutées au processus d'affaire.
- Prévoir un processus de révision périodique des procédés;
- Un organisme public peut sans le consentement de la personne concernée, communiquer un ficher de renseignements personnels (pour coupler, comparer, apparier) si cette communication est nécessaire à l'application d'une loi au Québec. Cela doit se faire dans le cadre d'une entente écrite, approuvée par la CAI (Commission d'accès à l'information) ou du gouvernement. L'entente doit mentionner les moyens mis en œuvre pour assurer la confidentialité[33];
- Planifier l'établissement et la gestion des fichiers: tout renseignement nominatif doit être versé dans un fichier de renseignements personnels ayant fait l'objet d'une déclaration à la CAI. L'organisme public doit s'assurer que les documents qu'il conserve sont à jour, complets et exacts pour servir aux fins auxquels ils sont destinés.

Notons que les « *renseignement personnels qui ont un caractère public* » ne bénéficient pas de la protection accordée aux renseignements nominatifs. Il s'avérera tout de même important de faire des choix judicieux en regard de l'utilisation de ce type d'information afin de respecter la finalité pour laquelle ces renseignements ont été rendus publics et ce, tout au long du cycle de vie de l'information.

3) Loi sur l'administration publique (PL 82)

[33] Cette façon de faire permettra si une liste est obtenue de l'externe, de s'assurer ou de présumer que toutes les autorisations requises ont été données.

Cette loi détermine le cadre de gestion de l'administration gouvernementale pour les ministères et organismes qui fournissent des services aux individus. Ainsi, les ministères et organismes qui fournissent directement des services aux individus doivent effectuer une déclaration de leurs objectifs quant au niveau et à la qualité des services qu'ils rendent et établir un plan stratégique et rendre compte des résultats atteints dans un rapport annuel de gestion (imputabilité devant l'Assemblée Nationale).

Quoique la liste ci-dessous ne soit pas directement liée à la sécurité de l'information numérique, les intervenants responsables de la sécurité de l'information numérique devront s'assurer que les mesures en cette matière permettront de :

- S'assurer que les informations (mesures) requises pour produire les comptes-rendus et les rapports annuels seront disponibles et traitables par les ressources responsables de la préparation des documents;
- S'assurer que les règles et les procédures qui régissent la prestation électronique de services sont simplifiées le plus possible (au bénéfice de l'individu) et que les technologies mises en place sont transparentes (au maximum) aux yeux des utilisateurs qui bénéficient d'une PES;
- Comme cette loi a comme priorité la qualité des services rendus aux individus, s'assurer que cette priorité se reflète dans le projet;
- S'assurer que les indicateurs de gestion seront produits et disponibles pour permettre l'atteinte des résultats en fonction des objectifs établis et l'évaluation de la performance du M/O;
- S'assurer de disposer des outils pour supporter l'accomplissement des conventions de performance et d'imputabilité;
- S'assurer que les dispositions du chapitre III sur la « Gestion des ressources humaines » sont respectées notamment dans le cadre de l'implantation de projets;
- S'assurer que les dispositions prévues relativement à la gestion des contrats et des ressources matérielles sont respectées, dont l'utilisation des informations inscrites au répertoire identifiant les catégories de biens, les catégories de services et les spécialités des fournisseurs;
- S'assurer que les dispositions relatives à la gestion budgétaire des dépenses et des investissements sont prises en compte dans les projets gouvernementaux;
- S'assurer que la gestion des ressources informationnelles sont gérées de façon à utiliser de façon optimale les TI et les communications comme moyen de gestion des ressources humaines, budgétaires et matérielles;
- S'assurer que l'ASIN favorise la concertation entre les ministères et organismes et le partage de l'expertise et des ressources.

4) Loi concernant le cadre juridique des technologies de l'information (PL 161)

Cette loi a pour objet d'assurer la sécurité juridique des communications effectuées au moyen de documents, l'équivalence fonctionnelle des documents et la reconnaissance de leur valeur juridique, quels qu'en soient les supports, ainsi que l'interchangeabilité de ces derniers. Il vise également à assurer la concertation en vue d'harmoniser les systèmes et les normes techniques permettant la communication au moyen de documents technologiques. Les aspects importants à considérer dans le cas d'une ASIN sont les suivants :

- Vérifier si le gouvernement a élaboré une réglementation connexe;
- Assurer l'intégrité des documents et le maintien de celle-ci tout au cours du cycle de vie;

- S'il y a des intermédiaires sur les réseaux de communication, définir le partage des responsabilités ou à tout le moins s'assurer que les dispositions de cette loi sont reflétées dans les ententes ou contrats conclus;
- S'il y a utilisation de modes d'authentification de l'identité d'une personne qui communique au moyen d'un document technologique, s'assurer que :
  - Des mesures de protection de la vie privée ont été prévues;
  - Qu'ils respectent des normes et standards reconnus et avalisés par le comité multidisciplinaire (comité prévu par la loi concernant le cadre juridique des technologies de l'information).
- Si des services de certification et de gestion de répertoire sont prévus, s'assurer que les dispositions de la loi sont respectées :
  - Accréditation;
  - Exigences minimales;
  - Utilisation des normes et standards reconnus et avalisés par le comité multidisciplinaire.
- Vérifier si le comité multidisciplinaire a fait des recommandations sur les normes et standards techniques utilisés dans le marché relativement au projet en question;
- S'assurer que les décisions prises en regard des dispositions de cette loi n'entrent pas en conflit avec d'autres lois telles les lois d'accès à l'information visant notamment la protection des renseignements personnels, la loi sur la protection du consommateur, la loi sur l'administration publique et le code civil (règles de droit civil) pour n'en citer que quelques-unes.

Certaines dispositions pertinentes du Code civil du Québec (C.C.Q.)

Le Code civil du Québec contient les règles de base du droit commun au Québec. Il est constitué d'un ensemble de règles régissant les individus et les biens et énonce les principes généraux du droit applicable sur le territoire québécois.

En fonction de la mission de l'entreprise et des processus d'affaires mis en place, il faudra s'assurer que les règles de droit civil sont appliquées et respectées afin de maintenir la solidité juridique de l'ASIN implantée. Par exemple, le code prévoit :

- Des règles relatives au respect de la réputation et de la vie privée (à noter que les règles particulières à l'égard de la protection des renseignements personnels sont établies dans les lois d'accès décrites plus loin dans cette section);
- Des règles relatives à la capacité des personnes (majorité, tutelle, régimes de protection, personnes morales (constitution et existence légale) de contracter et d'exercer leurs droits civils, sont édictées et devront faire l'objet de considération dans certains projets. Les personnes doivent être aptes à transiger même dans leurs relations à distance. Pour ne citer que l'article 165 du C.C.Q. :

  « La simple déclaration faite par un mineur qu'il est majeur ne le prive pas de son action en nullité ou en réduction de ses obligations »

  On peut également citer l'exemple des mandataires de corporations qui doivent avoir les autorisations et procurations requises pour dûment représenter le mandant.

  Cette disposition doit donc inciter les intervenants impliqués dans l'élaboration de l'ASIN, à mettre en œuvre des mécanismes de vérification et de validation de la capacité dans les circonstances appropriées.
- Des règles en matière de contrat portant notamment sur :

- Les conditions de formation du contrat;
- Le consentement
- L'objet du contrat : celui-ci devant être licite;
- La forme du contrat : noter que dans certains cas précis une forme particulière ou solennelle est requise;
- L'identité des parties (existence légale);
- Le paiement : noter ici que le paiement doit être fait au créancier ou à une personne autorisée à le recevoir et que les paiements doivent être faits avec des avoirs sur lesquels la personne a le droit de « donner en paiement » (par exemple, le signataire du compte bancaire peut signer adéquatement le formulaire d'inscription au prélèvement automatique). Le débiteur qui paie a droit à un reçu (cela devra donc être prévu dans les fonctionnalités des systèmes informatiques);

- Des règles relatives aux obligations en général;
- Des règles relatives au droit de la preuve;
  - Moyens de preuve;
  - Recevabilité des éléments et des moyens de preuve;

  Notons que la loi concernant le cadre juridique des technologies de l'information contient également des dispositions relatives aux notions de preuve des documents.

  Prévoir, le cas échéant, la possibilité d'établir la Date-Heure-Minute (DHM) et la production d'accusés-réception afin de disposer de moyens de preuves supplémentaires (notamment à travers des mécanismes de notarisation).

- Des règles relatives au droit de la prescription : notez que les règles de prescriptions conditionneront les durées de conservation de certaines informations numériques.

Loi sur la protection des renseignements personnels dans le secteur privé (L.R.Q., ch. P - 39.1)

Cette loi s'applique à des documents détenus par des **organisations privées** contenant des renseignements personnels, quel que soit le support de ces renseignements. Cette loi ne s'applique pas à un organisme public au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Cependant, les intervenants impliqués dans la définition de l'ASIN devront s'assurer que les partenaires d'affaires et fournisseurs des M/O respectent cette loi en ce qui concerne les liens d'affaires les unissant. Ainsi, le M/O devra s'assurer :

- Que ses partenaires ont mis en place les procédures et mécanismes de sécurité visant à assurer le respect de la législation et à assurer la confidentialité des renseignements (soient ceux qui sont impliqués dans la solution de sécurité);
- Que les informations numériques reçues de ses partenaires ont fait l'objet des déclarations, autorisations, consentements requis aux fins de cette loi;

- Que des contrats et ententes seront mis en place pour garantir une norme élevée de sécurité (par exemple, les données transmises et utilisées le seront seulement aux fins du contrat passé entre les deux organisations)[34].

Loi sur la protection des renseignements personnels et les documents électroniques (C-6)

Cette loi canadienne balise la gestion des renseignements personnels et touche principalement la protection de l'information et des renseignements personnels dans le contexte du commerce électronique dans les activités commerciales. Elle s'applique à toute organisation : entreprise, association, société de personne ou syndicat. Elle entre en vigueur selon le calendrier suivant : 1er janvier 2001 pour les organisations du secteur privé réglementées par le gouvernement fédéral et pour le commerce de renseignements personnels à l'échelle internationale et interprovinciale. À partir de janvier 2004, son application sera élargie aux activités internationales et interprovinciales de données personnelles (collecte, utilisation, communication).

Les organisations relevant de la compétence provinciale et les transactions conclues à l'intérieur de la province sont soustraites à l'application de cette loi. Elles sont plutôt assujetties aux lois provinciales.

Les intervenants impliqués dans l'élaboration de l'ASIN doivent considérer en regard de cette loi :

- Si la solution mise en place implique des transactions de nature « commerciale » extra provinciales, il faudra, le cas échéant, s'enquérir de la portée de cette loi sur le projet.
- S'assurer que les dispositions des lois d'accès québécoises sont respectées.

Loi sur le droit d'auteur (L.R. 1985 ch. C-42)

Le droit d'auteur est un droit de propriété intangible qui s'applique à plusieurs biens dont les logiciels, multimédia, le cédérom et les bases de données. L'enregistrement du droit d'auteur est facultatif au Canada et il présume de la protection de l'œuvre et de la titularité du droit d'auteur dans cette œuvre en faveur du nom y apparaissant. En vertu de la Convention de Berne, tous les droits protégés dans un état membre le sont dans les autres états membres de la Convention.[35]

Les intervenants impliqués dans les aspects juridiques de l'élaboration de l'ASIN devront vérifier :

- L'existence de droits d'auteurs assortis notamment d'exclusions, de limitations et d'exceptions comprenant la production, la reproduction, la publication, l'adaptation et la traduction des œuvres;
- S'assurer qu'il n'y a pas de violation aux droits d'auteurs;
- La nécessité d'obtenir une cession de droit ou une licence pour un cas précis en tenant compte des périodes de temps requises;
- Faire les vérifications relatives aux droits d'auteurs s'il y a des logiciels protégés qui doivent être copiés ;
- S'assurer que tous les aspects des droits pertinents ont été affranchis (par exemple pour l'obtention des licences nécessaires).

[34] Cette façon de faire permettra, si une liste est obtenue de l'externe, de s'assurer ou de présumer que toutes les autorisations requises ont été données.
[35] Tiré du document *Le droit d'auteur au Canada – Bases*, sur le site des Publications du Québec.

Il est à noter que les programmes d'ordinateur peuvent faire l'objet d'un droit de location depuis 1997.

Lois sur la propriété intellectuelle et les marques de commerce (L.R. 1985 ch. T-13)

Ces lois peuvent aussi être des éléments à considérer dans le cadre de l'évaluation de la dimension juridique de l'ASIN. À titre indicatif, les intervenants impliqués devront :

- Effectuer les recherches appropriées auprès des registraires ou de professionnels pour repérer les droits qui sont déjà protégés afin de ne pas les utiliser illégalement ou entrer en contact avec les organismes qui gèrent les droits;
- Vérifier la durée de la protection des droits;
- Le cas échéant, obtenir les cessions de droits ou de propriété de la part du titulaire des droits;
- S'assurer auprès des organismes de gestion et des producteurs que tous les aspects des droits ont été affranchis sinon voir à la préparation d'un contrat d'affranchissement;
- Si une marque doit être protégée (pensons aux logos, noms, noms de domaines, sons, secrets industriels, protection des textes et logiciels, brevets etc.), ils devront prévoir l'enregistrement requis auprès des institutions compétentes.

Lois sectorielles

Certains ministères et organismes et même des partenaires d'affaires sont assujettis à des lois et règlements spécifiques régissant leurs activités. Les intervenants impliqués dans l'élaboration d'une ASIN, devront considérer lors de la conception des projets :

- L'analyse des différentes lois (et règlements) applicables au domaine ou secteur d'affaires afin de repérer les dispositions pouvant avoir un impact sur l'élaboration de l'ASIN. Par exemple, un projet impliquant le secteur de la santé et des services sociaux, devra nécessairement passer par une analyse minutieuse et rigoureuse de la *Loi sur la santé et les services sociaux* et peut-être même d'autres lois telles la *Loi sur l'assurance maladie*, la *Loi sur l'assurance médicaments*, la *Loi sur les accidents du travail et les maladies professionnelles* et ainsi de suite;
- L'intégration de l'ASIN aux contraintes imposées par les différentes législations sectorielles;
- La nécessité ou non de faire amender, modifier ou abroger certaines dispositions restrictives à l'égard du projet.

2.4.1.2 La Charte des droits et libertés de la personne (C-12) et la Charte canadienne des droits et libertés

Les chartes touchent les libertés et droits fondamentaux de la personne : sauvegarde de la dignité, de l'honneur et de la réputation. Elles rappellent aussi le droit au respect de la vie privée, au secret professionnel, au droit à l'égalité et à la liberté d'expression.

Les facteurs juridiques liés aux Chartes ont préséance sur toute autre loi. Les différents intervenants dans les projets liés aux affaires électroniques devront veiller à respecter les dispositions de ces Chartes.

2.4.1.3 Les contrats, ententes et conventions :

Les contrats, ententes et conventions sont une source de droits et d'obligations à considérer dans le cadre de projets d'élaboration d'une ASIN. Entre autres, il faut :

- Vérifier les liens contractuels :
  - Adapter si nécessaire et possible les ententes contractuelles déjà en vigueur avec les partenaires d'affaires;
  - Adapter si nécessaire et possible les contrats ou demandes d'adhésion;
  - Réviser les ententes avec les fournisseurs de services (responsabilités qui leur incombent et maintien du niveau de sécurité requis);
  - Prévoir lorsque requis la préparation d'une entente entre M/O pour l'échange ou le partage de l'information numérique de façon à respecter les dispositions de la *Loi d'accès aux documents des organismes publics et sur la protection des renseignements personnels*;
- S'assurer que les contrats, lorsque requis, contiennent : une description détaillée des services, des clauses de résiliation et de modification, des clauses techniques et particulières aux services offerts, la durée du contrat, les modalités d'application diverses, des clauses d 'assistance diverses, des clauses monétaires, des clauses relatives à la sécurité et à la protection de la vie privée, des clauses relatives au traitement accordé aux renseignements personnels reçus, des clauses relatives à la responsabilité des parties (engagement de certains tiers lorsque requis - cautionnement - lettre de garantie etc.), les clauses relatives à la propriété intellectuelle, les clauses relatives à la juridication (choix du for, clause d'arbitrage), etc.;
- Faire analyser par des personnes compétentes les clauses de non-responsabilité (attention aux lois d'ordre public et aux dispositions spécifiques de d 'autres pays);
- En ce qui concerne le contenu d'un site WEB, les enjeux juridiques suivants sont à considérer pour la conception de l'ASIN :
  - Problèmes de preuves potentielles, lieu de formation du contrat; « Clicwrap », identification des parties, contrats d'adhésion, sécurité des transactions et des paiements, problèmes d'exécution des jugements, homologation des jugements, recours à l'arbitrage.

2.4.1.4 Autres considérations d'ordre juridique

Pour les intervenants impliqués dans la conception d'une ASIN, il s'avère important de regarder tout le contexte juridique qui doit s'appliquer. Ainsi, sans en faire une liste exhaustive, il pourra être recommandé de s'interroger sur les autres considérations suivantes :

- Le Consentement :
  - ***Manifeste*** (expresse ou tacite) de la volonté d'une personne d'accepter certaines conditions (d'un contrat, d'une entente, d'un échange d'informations, etc.). Ce point amènera les intervenants à réfléchir sur la validité de la signature numérique ou du simple « clic » sur un bouton d'envoi;
  - ***Libre et éclairé***. Le consentement qui porte sur la nature du contrat, sur l'objet de la prestation ou sur tout autre élément essentiel ayant déterminé le consentement est vicié si une erreur à ce sujet est survenue. Le consentement peut également être vicié par la crainte ou la lésion.

    Notons que le consentement donné à des fins spécifiques et pour une durée nécessaire à la réalisation des fins pour lesquelles il a été demandé dans le cas de la PRP est aussi rattaché à la valeur de celui-ci.

- L'application du code criminel, notamment pour les infractions et pénalités;
- Les lois fiscales;
- Le droit de la concurrence :
  - S'assurer de ne pas faire de représentations trompeuses ou de fausses représentations;
- La Loi de protection du consommateur s'il y a transaction entre un commerçant et un consommateur;
- La Charte de la langue française : les ministères et organismes québécois ont le devoir et l'obligation de jouer un rôle exemplaire dans l'application et la promotion de la langue française au Québec. Ils ont le devoir d'appliquer la politique et la Charte de la langue française.
  - S'assurer de l'usage de la langue française et de la qualité de celle-ci dans les différentes composantes du projet : pages Web, documentation, formulaires électroniques, guides d'utilisation, support technique, certificats, attestations, permis, clauses, contrats d'adhésion, communications de tous ordres, etc.;
  - Sauf certaines exceptions prévues à la législation, tout logiciel, y compris tout système d'exploitation (installé ou non) doit être disponible en français à moins qu'il n'existe aucune version français.
- Le respect de la législation et de d'autres sources de droit en vigueur (codes, lois, règlements, directives, politiques, décrets, tarifs, arrêtés en conseils);
- Exigences minimales émanant d'organismes gouvernementaux responsables de l'élaboration de règles de domaines sous leur juridiction.

2.4.2 Dimension humaine

La présente section présente un découpage des principaux aspects de la sécurité touchant la dimension humaine. Le contenu de celle-ci a été tiré principalement du *Manuel canadien de la sécurité des technologies de l'information* et de la *Norme de sécurité technique des TI* de la GRC[36]. Les différents points qui y ont été intégrés sont ceux qui ont été jugés les plus saillants mais la liste ne s'avère aucunement exhaustive vu le grand nombre et la multiplicité des situations que peuvent rencontrer les différentes organisations individuellement. Celle-ci se veut plutôt un guide visant à stimuler la réflexion des différents intervenants responsables du développement et de la mise en œuvre d'une architecture de sécurité de l'information numérique (ASIN).

2.4.2.1 L'aspect de la sécurité du personnel

L'organisation de la sécurité informatique passe nécessairement par la structuration et la définition de politiques de sécurité en regard de son personnel. Celles-ci devraient notamment couvrir les aspects liés à :

- L'enquête de sécurité;
- L'habilitation sécuritaire du personnel;
- La sensibilisation à la sécurité dans l'organisation;
- La formation.

[36] On se référera à la *Norme de sécurité technique des TI* de la GRC et au *Manuel canadien de la sécurité des technologies de l'information (MG9)* pour plus d'informations.

Enquête de sécurité

Lors de la nomination du personnel ou lors du rattachement à un rôle lié à la gestion de la sécurité, il peut s'avérer nécessaire de réaliser une enquête de sécurité (dont la portée devra être définie dans une politique de gestion du personnel) afin de s'assurer que les personnes choisies ont le profil, l'honnêteté et la fiabilité requis pour être dotées de telles responsabilités. Il faudra avoir défini dans un cadre de gestion de la sécurité la portée de l'enquête, la nécessité de celle-ci et les modalités d'exécution (aval des syndicats, consentement des personnes, etc.).

Habilitation sécuritaire

L'habilitation est la capacité qui est accordée à une personne d'accomplir un acte ou une fonction. Cette habilitation doit être spécifique et établie en fonction notamment du rôle, des systèmes ou des informations auxquelles la personne aura accès. Lorsque requis, cette exigence est valable pour tous les employés, individus, entreprises et autres clientèles ayant accès aux systèmes, infrastructures ou informations numériques. Les principales étapes de réalisation d'une habilitation sécuritaire sont :

- Définir dans une politique de sécurité les règles concernant les habilitations et les responsabilités[37];
- Définir la sensibilité associée (niveau de confiance) au poste en fonction de différents facteurs préalablement établis (opération délicate);
- Accorder à chaque rôle un ou des privilèges appropriés (règle du moindre privilège) [38] (accès donné selon les besoins). Considérer également les habilitations qui peuvent être requises pour les différentes clientèles;
- Associer à chaque rôle, l'utilisateur ou la ressource dont le profil correspond. Sensibiliser et informer ces personnes en conséquence;
- Tenir une liste actualisée des habilitations;
- Planifier comment les changements d'habilitation (transferts, affectations temporaires, départs amicaux ou inamicaux) seront gérés;
- Effectuer une gestion adéquate des habilitations dans le cours normal des opérations[39].

Sensibilisation à la sécurité

La sensibilisation du personnel et des clientèles aux différents risques informatiques, aux erreurs, aux malveillances et aux différents impératifs de sécurité vise notamment à développer un sentiment de responsabilité à l'égard de la sécurité à l'intérieur de l'organisation et à renforcer l'ASIN mise en œuvre. Elle permettra également, dans le cas du personnel, le rehaussement de leur pratique professionnelle et par conséquent leur degré d'imputabilité. Les principales activités à considérer dans le cadre d'un programme de sensibilisation sont:

[37] Se doter d'un responsable de la sécurité de l'information numérique (RSIN), d'un coordonnateur de la sécurité, d'un responsable de la sécurité des communications et autres responsables pour la sécurité du personnel, du milieu, des logiciels et du matériel, des opérations.

[38] N'accorder aux utilisateurs que les autorisations d'accès (logiques et physiques) dont ils ont besoin pour effectuer leurs tâches officielles (Tiré du manuel canadien de la sécurité des technologies de l'information).

[39] Par exemple, s'assurer qu'une personne ne soit pas seule responsable d'une fonction vitale ou d'un processus essentiel.

- Établir et exécuter un programme de sensibilisation à la sécurité portant notamment sur l'ensemble des dispositifs de sécurités, des faiblesses, des préoccupations et des procédures.
- S'assurer que tout le personnel et les clientèles y ont accès[40]. Chaque employé et chaque utilisateur devrait avoir pris connaissance des politiques de sécurité et de la documentation afférente et idéalement reconnaître de façon expresse l'avoir reçue, l'avoir comprise et s'engager à la respecter;
- Organiser les processus de travail de façon à accroître la sécurité et attribuer des tâches spécifiques concernant la sécurité et à sa promotion;
- Diffuser les informations relatives à la sécurité et aux résultats de l'application de celle-ci;
- Après une campagne de sensibilisation, redonner de l'information périodiquement;
- Combiner l'information visant la sensibilisation à celle concernant le contrôle de la sécurité.

Formation du personnel

Un plan de formation doit être élaboré de façon à ce que chacun reçoive une formation adéquate en ce qui a trait à la sécurité dans l'organisation. Cette formation[41] doit être adaptée au rôle que chacun occupe en regard de la sécurité (personnel responsable de la gestion de la sécurité, gestionnaire de système, usager) et devrait idéalement être personnalisée pour chacun des groupes ciblés. La formation doit notamment porter sur :

- Les politiques de sécurité
- Le cadre de gestion de la sécurité (principes, règles et procédures);
- Les dispositifs de sécurité et les privilèges d'accès;
- Le plan de relève;
- Les faiblesses des systèmes;
- Les renseignements sensibles auxquels ils ont accès (responsabilité relativement à PRP et informations de nature délicate);
- Les lois applicables.

Le programme de formation doit être tenu à jour et évoluer avec l'ASIN. Le personnel doit recevoir un perfectionnement sur les nouvelles mesures afin d'assurer l'efficacité de l'ASIN et l'imputabilité du personnel.

2.4.2.2 Éthique, pratique professionnelle et imputabilité

Ces notions impliquent l'ensemble des individus de l'organisation depuis la haute direction jusqu'à l'utilisateur final. Tous ont des obligations en regard de l'organisation, lesquelles visent le maintien de la crédibilité et de la renommée de l'organisation, le maintien de la confiance des clients, le maintien de la qualité des services aux clients, le maintien de la productivité des employés et la diminution des pertes financières qui passent par le maintien des notions d'éthique, de pratique professionnelle et d'imputabilité.

[40] Formation, avis, documentation, vidéos, séances d'information + attestation de prise de connaissance ou présence à l'appui si formation.
[41] Formation en salle, avis, documentation, vidéos.

Les quelques exemples qui suivent permettront au lecteur de mieux comprendre comment ces notions peuvent être gérées à l'intérieur d'une ASIN.

- Les responsabilités de l'organisation sont de :
  - Former et sensibiliser son personnel et ses clientèles;
  - Éduquer en regard de la sécurité des technologies de l'information afin d'améliorer les actes et comportements des êtres humains à l'intérieur de l'organisation et à rehausser la qualité de leurs interventions;
  - Se doter d'une structure décisionnelle efficace et représentative.
- Les responsabilités des gestionnaires sont de :
  - S'assurer que la haute direction s'approprie la politique de sécurité et donne l'exemple;
  - Obtenir des consentements valables et des déclarations à l'effet que les employés ont bien compris et connaissent les impératifs de sécurité liés à leur habilitation;
  - Réagir en temps opportun aux incidents, de façon uniforme et donner de la rétroaction;
  - Démontrer un comportement exemplaire et insister sur l'importance des différentes dimensions de la sécurité;
  - Mettre en place des mécanismes et des produits facilitants pour le personnel et les clientèles en regard de la sécurité afin d'éviter la confusion et la mauvaise compréhension.
- Les responsabilités du personnel et des clientèles sont de :
  - Prendre connaissance des exigences et prérogatives liés à son habilitation afin d'assumer adéquatement la responsabilité de ses actes;
  - Reconnaître (prendre conscience) que les actes frauduleux, les erreurs et les omissions sont des pratiques qui mettent en péril la sécurité de l'organisation;
  - Comprendre clairement sa responsabilité en matière de protection des données et des renseignements, de protection des logiciels protégés par les droits d'auteurs, des conditions de maintien de son profil d'usager et autres;
  - Agir avec prudence et diligence pour obtenir les résultats envisagés;
  - S'informer, demeurer à jour et rechercher l'information auprès de la haute direction et des responsables de la sécurité de la sécurité de l'information numérique;
  - S'assurer de maintenir toutes les conditions accessoires relatives à l'obtention de leur profil (accréditation professionnelle, résidence…)

2.4.3 Dimension organisationnelle

La dimension organisationnelle d'une architecture de sécurité de l'information numérique (ASIN) s'articule ici sous les aspects plus spécifiques de la sécurité administrative, de la sécurité physique et environnementale et de la sécurité des opérations. Le contenu de la présente section se veut une extraction des points saillants d'ouvrages et de documents plus détaillés et approfondis en la matière[42] auxquels le

[42] On se référera à la *Norme de sécurité technique des TI* de la GRC et au *Manuel canadien de la sécurité des technologies de l'information (MG9)* pour plus d'informations.

lecteur pourra se référer pour se préparer à un exercice plus exhaustif d'élaboration d'une politique de sécurité et d'un cadre de gestion de la sécurité[43].

2.4.3.1 L'aspect de la sécurité administrative

L'aspect de la sécurité administrative peut être traité différemment d'une organisation à une autre sous la réserve des règles que le CT peut imposer sur la sécurité en vertu du chapitre IV de la Loi sur l'administration publique. Les sous-points suivants sont cependant ceux qui ont un caractère prépondérant dans le cadre de l'analyse qui nous concerne et sur lesquels il faut porter une attention particulière dans le respect des règles, politiques et directives gouvernementales adoptées :

- Politiques, normes, standards et directives de sécurité;
- Rôles et responsabilités du personnel chargé de la sécurité;
- Catégorisation de l'information;
- Analyse de risque et évaluation de vulnérabilité;
- Registres et dossiers de sécurité;
- Gestion du consentement;
- Prévention.

Notons que la structure documentaire présentée ci-dessus est à titre indicatif seulement. Il existe de multiples autres structures documentaires portant sur l'aspect administratif de la sécurité. Les M/O devront analyser leurs besoins en la matière et mettre en place une structure appropriée basée sur le Modèle de gestion de la sécurité des systèmes d'information dans l'Administration québécoise[44].

Politiques, normes et directives de sécurité

L'objectif principal de la politique de sécurité est d'énoncer les dispositions du cadre général régissant la gestion de la sécurité et la protection des informations numériques (et papiers). La politique de sécurité contient principalement les lignes directrices établies par la haute direction en rapport avec la création d'un programme de sécurité en technologies de l'information. Il est aussi possible d'établir des politiques de programmes, des politiques propres à une question et des politiques propres à une TI.

- La politique générale du M/O devrait comprendre:
  - Un objet qui exprime la volonté de la haute direction de mettre en place une infrastructure de sécurité, le cadre d'application et les principaux buts de celle-ci;
  - La portée du champ d'application de la politique (quels usagers, les classes d'usagers, quels actifs informatiques, quelles informations – Qui? Quoi? Comment? Où?);
  - Les responsabilités des différents groupes d'usagers et de gestionnaires et l'assignation de celles-ci;

[43] On se référera au *Recueil des pratiques recommandées en matière de sécurité de l'information numérique* publié par le SCT en décembre 1999 pour plus d'informations.

[44] On se référera au *Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise* (février 2001) basée sur la norme ISO/IEC 13335 produit par le SCT pour plus d'informations.

- Les dispositions sur le respect de la politique et le traitement des contraventions[45];
- Les principes directeurs ou normes organisationnelles relativement à des aspects de sécurité dont notamment la confidentialité, la protection des installations et équipements informatiques; l'utilisation des systèmes informatiques et autres;

- Une politique propre à une question devrait comprendre : un énoncé de la question, la position de l'organisation, l'applicabilité, les rôles et responsabilités, le respect de la politique, les points de contact et d'information supplémentaire. Elle peut notamment porter sur :
  - Internet et le courriel;
  - Le télétravail;
  - Les droits d'accès et la gestion des profils des usagers;
  - La conservation (Comment? Où? Combien de temps?).
- Une politique propre à une TI devrait comprendre : les objectifs de sécurité, les règles opérationnelles et de mise en œuvre;
- Un cadre de gestion de la sécurité comprenant notamment des normes, directives, guides, procédures, etc. doit être élaboré pour donner une dimension plus détaillée et spécifique (le comment?) aux dispositions des différentes politiques afin de permettre leur mise en application;
- Les notions intégrées à ces documents (politiques, normes, directives, guides, procédures, etc.) doivent être claires et faciles à comprendre et adaptées au degré de contrôle ou de sécurité requis;
- Une personne (ou instance ou groupe) responsable doit être identifiée pour les fins d'interprétation des politiques, leur mise à jour, leur diffusion auprès des nouveaux arrivants et leur révision périodique;
- Les politiques et le cadre de gestion de la sécurité doivent être diffusés, mis à jour périodiquement et être conservés et disponibles pour consultation afin de permettre l'atteinte des objectifs d'imputabilité administrative et juridique.

Rôles et responsabilités du personnel chargé de la sécurité

- L'organisation doit se doter de personnel chargé de la gestion de la sécurité et définir les rôles et responsabilités appropriés à l'organisation. Au niveau des M/O, les principaux acteurs de la sécurité sont[46] :
  - Sous-ministre;
  - Comité de la sécurité;
  - Responsable de la sécurité de l'information numérique (RSIN);
  - Détenteurs des systèmes d'information;
  - Responsables de la gestion documentaire;
  - Responsables de l'accès à l'information et de la PRP;
  - Gestionnaires;
  - Services informatiques;
  - Utilisateurs;
  - Direction des TI.

[45] Les politiques, normes et directives doivent être appliquées uniformément.
[46] On se réfèrera au *Recueil des pratiques recommandées en matière de sécurité de l'information numérique : Partie 1 – Gestion de la sécurité* publié par le SCT pour plus de détails sur les responsabilités de ces acteurs.

- Des M/O ont des fonctions particulières à l'égard de la gestion de la sécurité: Conseil du trésor, Secrétariat du Conseil du trésor, ministère de la Justice, ministère des Relations avec les citoyens et de l'Immigration, Conservateur des Archives nationales, Sûreté du Québec et Contrôleur des Finances[47]
- De façon générale, les groupes suivants[48] sont aussi concernés par la sécurité des technologies de l'information : Haute direction, groupe de gestion de la sécurité, propriétaires d'applications, fonctions de soutien, responsables des approvisionnements, responsables des ressources humaines, etc.
- Les fournisseurs doivent aussi se préoccuper des rôles et responsabilités du personnel chargé de la sécurité dans leur organisation lorsqu'ils font affaires avec le gouvernement du Québec.
- Les responsabilités de chacun doivent être clairement définies et attribuées en fonction du rôle joué dans l'organisation en regard de la sécurité. Cette condition est nécessaire à l'imputabilité du personnel et des usagers.

Catégorisation de l'information

La catégorisation de l'information permet d'élaborer et de mettre en place des mesures, mécanismes de sécurité et solutions technologiques adaptés aux besoins de l'organisation. Elle nécessite un inventaire des informations et documents impliqués dans chacun des processus d'affaires.

Le « Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité » du SCT explique le contexte et la démarche pour catégoriser l'information numérique et établir les mesures de sécurité à mettre en place selon le contexte d'utilisation. Il définit les étapes liées spécifiquement à la catégorisation de l'information numérique, soit[49] :

1. Décider de l'information à catégoriser :

   Les informations numériques à catégoriser sont celles enregistrées, emmagasinées et échangées de façon électronique et dont un ministère ou un organisme doit se préoccuper pour les sécuriser. Ainsi, il n'est pas nécessaire d'appliquer une catégorisation sur toutes les informations et un regroupement de celles-ci est fortement recommandé pour simplifier l'exercice de catégorisation.
2. Catégoriser ces informations :

   Les éléments à catégoriser retenus font l'objet d'une évaluation sur les attributs qui font partie des principes directeurs de la directive, communément désignés sous le vocable DICAI. On y précise également leur contexte d'utilisation puisque pour une même information, les mesures de sécurité peuvent effectivement varier selon le contexte.
3. Déterminer les mesures à appliquer pour protéger les informations en fonction de la catégorisation désirée :

   La dernière étape consiste à prendre en considération les mesures généralement appliquées en fonction du contexte d'utilisation et du niveau de catégorisation retenu à l'étape précédente pour assurer un niveau acceptable de sécurité

Ce guide devrait être utilisé comme base à toute activité de catégorisation de l'information par les ministères et organismes.

[47] On se réfèrera au *Recueil des pratiques recommandées en matière de sécurité de l'information numérique : Partie 1 – Gestion de la sécurité* publié par le SCT pour plus de détails sur les responsabilités de ces acteurs.
[48] Tiré du *Manuel canadien de la sécurité des technologies de l'information*.
[49] On se référera au *Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité* pour plus de détails sur le processus de catégorisation de l'information.

Analyse de risque et évaluation de vulnérabilité

Tel que vu précédemment, le « Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité » spécifie une troisième étape liée à la détermination des mesures à appliquer pour protéger les informations en fonction de la catégorisation retenue. Selon ce guide, « il est préférable pour les ministères et organismes de réaliser un état de leur sécurité (évaluation de vulnérabilité) et une analyse de risques avant de passer à cette troisième étape[50] ».

L'évaluation de la vulnérabilité consiste à identifier ce qu'on souhaite protéger, à reconnaître ce dont on veut le protéger et à comprendre comment le protéger. Cette évaluation passe principalement par l'évaluation des menaces et des risques.

Le risque est la probabilité qu'une menace[51] se réalise (il faut donc connaître les menaces pour gérer les risques). Cette activité devrait également permettre de prendre les dispositions pour réduire la vulnérabilité à un niveau acceptable pour l'organisation, accepter les risques résiduels et à maintenir le niveau de risque à celui choisi par la haute direction et les gestionnaires.

Ces dispositions sont :

- Nécessité d'analyser et de bien connaître les besoins d'affaires de l'organisation et d'utiliser une grille d'analyse des informations et documents et de leur sensibilité (voir le Guide de catégorisation);
- Utiliser une méthodologie adéquate (offrant des thèmes et points à considérer);
- Faire l'identification des menaces : elles peuvent être de nature humaine (erreurs de conception ou exploitation, trafic d'information, sabotage et curiosité), de nature technologique (pannes) ou de nature imprévue (catastrophe naturelle);
- Analyser les mesures de protection potentielles, incluant des mécanismes de sécurité et des solutions technologiques;
- Estimer la vulnérabilité : faire l'interprétation des risques en faisant une sélection des informations et un classement des biens, des menaces et des vulnérabilités de façon à faciliter l'interprétation et consigner les résultats;
- Évaluer la probabilité : l'interprétation de l'analyse permettra de soutenir l'acceptation des risques et la sélection de mesures de protection présentant un bon rapport coût / efficacité[52];
- Mettre à jour l'évaluation suite à un changement dans le système, modification, ajout etc.

Il est à noter que la qualité[53] de l'analyse dépendra de la qualité du processus d'évaluation et de la qualité dans la sélection de l'information et dans l'interprétation des résultats obtenus. L'atténuation des risques dépendra de la sélection des mesures de protection, de l'acceptation des risques résiduels et de la mise en œuvre et du contrôle de l'efficacité des mesures de protection.

---

[50] *Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité*, p. 8

[51] Accès à des documents confidentiels par des personnes non-autorisées, altération d'information, destruction d'informations, modification de l'exploitation des ordinateurs pour les rendre inopérants ou disfonctionnels, récupération de logiciel de type portefeuille pour faire des transactions bancaires frauduleuses, accès non-autorisés aux données, coulage de renseignements privilégiés, interruption de fonctionnement ou d'accès, virus, fraude et usurpation d'identité, non-respect de la vie privée, diffamation, détournement de trafic d'un site WEB, etc.

[52] Tiré du *Manuel canadien de la sécurité des technologies de l'information*.

[53] Il existe plusieurs guides de référence et de méthodologies.

Registres et dossiers de sécurité

L'aspect de la sécurité administrative contient un volet relatif à l'établissement de registres et de dossiers de sécurité dans le but de supporter d'autres éléments de sécurité telles que la surveillance et l'audit, l'imputabilité, la gestion des mesures d'urgences et le contrôle de l'accès physique et logique.

Les dispositions à prendre à cet égard sont :

- Un cadre de gestion de la sécurité devrait inclure la gestion des registres et des dossiers de sécurité et être élaboré en fonction des besoins de l'organisation. Il devrait entre autres concerner le type de registres à mettre en place, les informations qui devraient y être consignées, le responsable de ceux-ci, leur conservation (durée et endroit), etc.
- Les registres doivent être tenus à jour et disponibles pour consultation par les personnes autorisées;
- Certains registres peuvent requérir une protection de confidentialité;
- Des registres doivent être tenus à jour relativement aux :
  - Responsables de la sécurité avec les habilitations correspondantes;
  - Utilisateurs avec les habilitations correspondantes;
  - Logiciels;
  - Informations;
  - Équipements;
  - Aux incidents de sécurité suite aux activités de surveillance et détection et des mesures prises;
  - etc.

Gestion du consentement

Lors du développement et de la mise en œuvre des différents processus opérationnels, les intervenants doivent se soucier d'informer les clientèles des caractéristiques particulières de sécurité des informations, formulaires, logiciels, systèmes ou dispositifs utilisés.

Par exemple, il s'avérera nécessaire de publier dans une application WEB des avertissements concernant la protection des renseignements nominatifs ou personnels, concernant les limitations d'usage des licences et autres avis ou mises en garde similaires.

Il faudra également se préoccuper de recevoir un consentement[54] valable (et de conserver celui-ci pour fin de preuve dans certains cas). En ce sens, les clientèles devront disposer de toute l'information et des mécanismes adéquats pour manifester leur consentement. On peut penser ici aux « clics » successif qu'un usager devra faire pour accepter une condition ou une clause d'utilisation d'un formulaire électronique.

Le consentement est généralement engendré par des besoins d'affaires ou des obligations légales. À cet effet, la gestion du consentement n'est pas considérée comme une fonction de sécurité.

Prévention

[54] La gestion du consentement fait l'objet d'un point particulier de recommandation dans le cadre de ce projet.

La prévention est l'un des aspects de l'administration de la sécurité qui ne doit pas être négligé. Elle permet notamment que les connaissances en matière de sécurité soient maintenues le plus à jour possible, elle permet de minimiser les risques encourus, elle permet d'être proactif plutôt que réactif, elle permet aux intervenants de maintenir leur vigilance et elle permet de corriger au bon moment une solution, de l'adapter à l'évolution des différents contextes et d'améliorer la sécurité de l'organisation.

La prévention, c'est faire de la sensibilisation marquée et continue auprès de tous les intervenants. Elle s'applique normalement à toutes les dimensions de la sécurité juridique, humaine, organisationnelle et technologique.

2.4.3.2 L'aspect de la sécurité physique et du milieu

La sécurité physique et du milieu vise principalement la sécurité du lieu physique (bâtiment, structure, le véhicule supportant le système tel un portable), la sécurité du lieu géographique (catastrophes naturelles, écologiques, cambriolage) et la sécurité des dispositifs auxiliaires (chauffage, électricité, climatisation).

Les paragraphes qui suivent traitent plus particulièrement :

- Des installations principales et auxiliaires aux ressources informationnelles;
- Du contrôle de l'accès physique;
- De la sécurité du matériel.

Installations principales et auxiliaires aux ressources informationnelles

La sécurité matérielle vise un ensemble de mécanismes de protection, de détection et de réponse utilisés dans l'environnement matériel (salles, portes, sites, accès, alarmes) pour contrôler l'accès aux biens et aux informations de nature délicate. Cet aspect implique la mise en place d'une politique et de procédures spécifiques à la sécurité physique et à la sécurité de l'environnement des installations et informations.

Les intervenants responsables de la mise en place d'une infrastructure de sécurité devront notamment :

- Choisir un emplacement à l'abri des risques : inondations, matières dangereuses, incendies;
- Prendre des mesures appropriées pour combler les lacunes relativement à l'emplacement choisi de façon à réduire au minimum les risques encourus (prévoir des constructions ou améliorations nécessaires le cas échéant);
- Utiliser des installations et des supports approuvés;
- Prévoir une protection suffisante des installations auxiliaires : électricité, chauffage, ventilation, climatisation selon les normes établies ou choisies (et s'assurer que tous ces systèmes sont installés et configurés conformément aux instructions du fabricant);
- S'assurer que les locaux auxiliaires et le matériel de réserve correspondent au moins au même niveau de protection que les installations principales (pour assurer les services essentiels);
- Veiller à l'installation du matériel informatique dans un lieu et sur des supports convenant à sa vulnérabilité;
- S'assurer que le tout, une fois installé, ne peut être déménagé sans autorisation (du responsable) ou sans le respect des mêmes règles;

- S'assurer qu'une personne responsable sera nommée pour effectuer des contrôles continus ou périodiques des installations et prévoir les modalités de signalement des écarts lorsque requis;
- S'assurer que les procédures d'entretien sont appropriées et sont faites selon les spécifications du fabricant;
- S'assurer de la consignation des activités d'entretien et des procédures de signalement et d'enregistrement des défectuosités (aussi du résultat final et des mesures prises);
- S'assurer que les informations ne peuvent être interceptées par indiscrétion, interception des transmissions de données et interception électromagnétique;
- S'assurer que les perturbations d'origine extérieure sont contrôlées : décharge statique, interférence, brouillage;
- Veiller à la mise en place de mesures de protection des systèmes portables.

Contrôle de l'accès physique

Le contrôle de l'accès physique vise la surveillance de l'accès lorsque requis. Le contrôle peut être fait de façon constante, sinon périodiquement.

Le contrôle de l'accès physique peut faire l'objet de politiques et de procédures. Les principaux axes du contrôle de l'accès physique sont :

- La surveillance par du personnel compétent, autorisé et adéquatement formé;
- La détermination de zones d'accès restreint devant être aménagées et disponibles pour recevoir ce qui est de nature délicate - salles d'ordinateurs, centres de télécommunications, bibliothèques, locaux divers, sites de relève…);
- L'accès aux zones qui est restreint, contrôlé, autorisé et surveillé en fonction du degré de protection requis :
  - Supervision du personnel d'entretien;
  - Insigne d'accès lorsque requis;
  - Moyens appropriés de contrôle d'accès (serrures, nombre minimum de points d'entrée, gardiens de sécurité, réceptionnistes);
  - Autorisation de l'accès : liste des personnes autorisées pour entrer dans les locaux et enregistrement des allées et venues;
- Registres d'accès tenus à jour avec toutes les informations requises pour faciliter les analyses rétroactives (dates et heures, zone, nom des personnes, employeur, etc.);
- Révision des registres de façon périodique;
- Conservation selon la période prévue dans les normes;
- Détermination des circonstances où l'accès physique peut être révoqué. Prévoir la récupération des articles de nature délicate : clés, insignes, documents etc.

La sécurité du matériel

La sécurité du matériel fait appel à différentes notions dont les principales sont :

- Tenue d'un inventaire du matériel (caractéristiques, numéros de série, modèle, etc.);
- Prévention;
- Surveillance;
- Détection;
- Entretien et soutien du matériel;
- Entretien préventif;
- Résolution de problèmes;
- Contrôle de la qualité : installations de soutien, contrôles des changements.

2.4.3.3 La sécurité des opérations

La sécurité des opérations fait appel à certaines notions de sécurité dont :

- La disponibilité: les clientèles doivent pouvoir compter sur les systèmes et les logiciels chaque fois qu'elles en ont besoin;
- Le contrôle : les gestionnaires concernés doivent être en mesure de savoir qui accède à quoi sur les systèmes et logiciels;
- La surveillance : les gestionnaires concernés doivent savoir qui fait quoi sur les systèmes et logiciels;
- L'archivage et le désarchivage, la saisie et le transfert des données, la sauvegarde, la maintenance;
- Le suivi de l'exploitation.

Les paragraphes qui suivent couvrent plus en détail la sécurité des opérations incluant :

- L'administration;
- Le contrôle d'accès logique;
- La surveillance et l'audit;
- L'utilisation et la gestion des supports;
- Les mesures d'urgence, de relève et de continuité
- La gestion des changements.

Administration

La sécurité dans les opérations passe par toute une série d'activités dont plusieurs sont sous la responsabilité des responsables de la sécurité de l'information numérique (RSIN). Ces activités d'administration peuvent se concrétiser notamment selon les différentes étapes de vie de l'information numérique. Des individus responsables de ces activités doivent être nommés afin d'établir les règles, de s'assurer que les opérations se font selon les processus établis, d'effectuer le contrôle et la supervision des

activités, de constituer et conserver les registres des activités d'entretien et de planifier des essais d'utilisation avec des ressources et du matériel appropriés.

Une bonne administration de la sécurité peut être garantie si les responsabilités de chacun sont clairement attribuées et consignées, si des contrôles d'uniformité et d'utilisation sont exécutés périodiquement et si des contrôles de confidentialité et d'intégrité sont réalisés.

Les différents responsables de la sécurité doivent s'assurer des points suivants :

- Détermination des besoins en sécurité et évaluation de la sensibilité de l'information numérique;
- Élaboration des spécifications en fonction des exigences de sécurité;
- Gestion des activités de développement;
- Acquisition de matériel, de logiciels, de locaux, etc. Cette activité exige que le gestionnaire intègre les exigences en matière de sécurité dans les contrats signés;
- Gestion des relations avec des organismes externes et des fournisseurs en fonction de la nature des informations ou des ententes signées;
- Paramétrisation et mise en œuvre du système en fonction des exigences minimales de sécurité, des mécanismes de sécurité et de solutions technologiques établis;
- Mise en place et activation des mesures de protection;
- Vérification de la sécurité et consignation des résultats et des écarts;
- Obtention d'accréditation lorsque requis;
- Consignation des normes et mise à jour périodique;
- Gestion des modifications aux opérations;
- Gestion de la documentation numérique, des informations et de la base de données: conservation, classification, archivage, conversion, élimination ou destruction;
- Entretien, prévention et résolutions de problèmes : procédures de signalement, de prise en charge, tenue de registres, etc.;
- Répartition des tâches : isolement des préposés aux opérations des usagers, répartition claire des tâches, répartition des tâches de contrôles de données, rotations lorsque requis, etc.;
- Gestion des affectations et des habilitations : lors de la mutation de personnel, procédures écrites afin que les privilèges soient modifiés. Lors de cessation d'emploi, procédures écrites sur ce qui concerne la sécurité après le départ (entente de confidentialité) et annulation des privilèges, mots de passe et autres.

Contrôle d'accès logique

Le contrôle de l'accès logique porte sur l'accès au système et l'autorisation. Il permet l'accès ou la limitation d'accès (le qui ? le quoi ? et le comment ?) en fonction de l'habilitation (identité, rôle), l'heure, l'emplacement, la transaction ou tout autre critère déterminé dans le cadre de gestion de la sécurité.

L'accès logique au système doit être supporté par une bonne politique et un cadre de gestion approprié[55] portant notamment sur :

- La nomination d'un administrateur de l'accès logique;
- Les modalités d'attribution d'un profil : protocole de création de mots de passe afin de s'assurer qu'ils sont conçus de façon sécuritaire et que leur confidentialité est assurée;
- Les protocoles de gestion des mots de passe et des identifiants;
- Les procédures de préparation, émission, modification, annulation et vérification des identifiants des usagers;
- Les modalités de révocation d'un profil : période maximum d'inactivité avant révocation;
- Les modalités d'accès : accès non permis tant que l'identification n'a pas été complétée avec succès (manuellement ou informatiquement), toute utilisation des installations informatiques préalablement autorisée, etc.;
- Les modalités d'accès distant : modes d'accès, types de connexion aux réseaux internes, restrictions concernant les types d'informations disponibles pour cet usager à distance;
- La tenue de registres portant sur les mécanismes d'authentification du système, des codes ou mots de passe utilisés (cote de protection la plus élevée);
- La gestion des autorisations ponctuelles;
- Les mécanismes et procédures mis en place afin de s'assurer que les accès aux systèmes et aux ressources seront respectés;
- Les autorisations pour sortir du matériel ou de l'équipement;
- La perte de privilège, une mesure disciplinaire ou des poursuites judiciaires suite à une infraction;
- La révision des processus et mécanismes d'enregistrement et de gestion des profils.

Surveillance et audit

La surveillance et l'audit sont des examens faits à intervalles réguliers (vérifications périodiques) ou ponctuellement (suite à un incident ou à une demande spécifique). Ils peuvent porter sur les programmes, les systèmes, les informations, les opérations et le personnel et devraient être réalisés tel que déterminé dans la politique de sécurité.

La surveillance et l'audit sont des activités supportées par des mécanismes de sécurité et des solutions technologiques [56] qui vont permettre normalement à l'organisation de déceler des incidents et de renforcer son infrastructure de sécurité de l'information numérique. La surveillance et l'audit vont également permettre de renforcer la sensibilisation et l'imputabilité des usagers et d'accroître la fiabilité du système et par conséquent la confiance que l'on peut accorder dans l'ASIN d'une organisation.

La liste suivante présente un certain nombre de points à considérer dans le cadre de la surveillance et de l'audit :

- Les activités à contrôler et les modalités de réalisation de celles-ci doivent être définies ;

[55] Lesquels doivent être divulgués, disponibles et diffusés.
[56] On consultera la section 2.5.7 pour plus de détails sur la fonction de surveillance.

- Un audit doit être exécuté après tout incident majeur de sécurité, un déménagement, une reparamétrisation, la modification des contrôles exercés sur les communications, sur la classification des informations, sur le mode d'exploitation, etc.;
- Un rapport des incidents décelés doit toujours être rédigé et la documentation sur la solution apportée au problème doit être produite;
- Des activités de suivi doivent être établies dans certaines circonstances, surtout lorsque la solution à un incident ou un problème n'est pas immédiatement implantée;
- Les résultats de la surveillance et des audits doivent être consignés et conservés selon le calendrier et les normes de conservation;
- Des registres et dossiers de sécurité contenant la liste des utilisateurs autorisés doivent être tenus à jour. Dans ces registres doivent également être consignés et signalés tous les incidents de sécurité (actions, délais et décisions);
- Les activités de surveillance et d'audit peuvent concerner les procédures d'exploitation (démarrage, comptes rendus de problèmes, mise sous et hors tension, entretien par l'opération, copies de sauvegarde, épuration du système, migration ou mise à niveau, récupération et relance), le contrôle des entrées et sorties, la surveillance et la détection des installations et systèmes, la tenue de registres, etc.
- Les activités de surveillance et d'audit doivent inclure une portion d'analyse des erreurs détectées (même celles des opérateurs) pour voir si elles mettent en péril la solution de sécurité.

Utilisation et gestion des supports

La gestion des supports (disquettes, bandes magnétiques, ordinateurs, disques durs, etc.) par une personne responsable et la détermination des procédures de gestion spécifiques sont essentielles à l'étanchéité de la solution de sécurité. Parmi les plus importantes activités de gestion des supports notons :

- L'identification de la valeur de l'information numérique sur les supports et dispositifs ainsi que les autres renseignements pertinents;
- La préparation et la tenue d'un inventaire selon le niveau de sécurité de ce qui est conservé dans le site et hors site;
- La tenue d'une bibliothèque des supports et registres;
- La détermination de mécanismes de protection contre l'écriture sur les supports, pour l'octroi d'une autorisation pour retirer un support d'une bibliothèque, etc.;
- La planification et l'acquisition des supports requis en cas d'urgence, des copies et du matériel essentiels pour la reprise des activités;
- La détermination des règles de disposition et de réutilisation des supports.

La disposition des supports d'information, qui concerne la destruction des supports d'information ainsi que la purge des supports d'information et de l'information elle-même, de même que l'envoi et le transport des supports, doivent tenir compte des éléments suivants :

- Si le support d'information contient des informations numériques de nature délicate, l'utilisation d'un processus approuvé de destruction devra être privilégié;

- Une protection adéquate doit être envisagée si un transport ou un déménagement quelconque est requis et que la destruction s'effectue dans un lieu autre que l'endroit où le support de l'information se trouve habituellement;
- Le personnel affecté aux différentes tâches du processus de destruction (manutention, transport, déchiquetage et autres) doit posséder le profil requis et les responsabilités afférentes;
- La surveillance peut être requise selon la sensibilité de l'information contenue sur le support;
- Les conditions de transport et modalités adéquates au niveau de sensibilité de l'information ou du document doivent être prévues;
- Lorsque requis, un registre de ces événements doit être établi et conservé.

Mesures d'urgence, de relève et de continuité

Les mesures d'urgence devraient normalement être identifiées dans le cadre de gestion de la sécurité. Les procédures d'urgence devraient être établies à l'intention des différents intervenants (qui contacter et dans quelles situations, étapes initiales d'interventions, rôles et responsabilités des membres de l'équipe d'intervention, informations à consigner, etc.) afin de bien encadrer cette activité de sécurité. La planification des mesures d'urgence permet l'encadrement des principales interventions visant le maintien des ressources critiques et la minimisation des impacts de l'incident[57].

Les mesures d'urgence, de relève et de continuité permettent de faire face aux imprévus et aux sinistres : défaillance majeure ou destruction, faillite d'un fournisseur, évacuation obligatoire d'un immeuble, perte d'un système de soutien essentiel, grève majeure. Ainsi :

- Les caractéristiques d'un bon dispositif de traitement contre les incidents sont :
  - Identification des activités fondamentales ou activités d'exploitation critiques;
  - Identification des ressources qui soutiennent les activités TI critiques et des contraintes de temps rattachées à ces fonctions (ressources humaines, applications, données, services, infrastructures physiques et documentation);
  - Prévisions des imprévus ou sinistres potentiels;
  - Sélection de stratégies (intervention d'urgence, récupération, reprise des activités);
  - Mise en œuvre des stratégies concernant les mesures d'urgence (documentation, formation);
  - Essais du plan d'urgence par une simulation d'un sinistre ou d'un incident (exercices pour tester la mesure d'urgence) et révision du plan en fonction des résultats obtenus et des écarts notés.
- Les mesures d'urgences ne doivent pas se cantonner dans la préparation d'un déménagement en cas de sinistre. Elles doivent également s'attacher au maintien des activités critiques de l'organisme en cas de perturbations;
- Le soutien pour le traitement des incidents doit également être planifié et organisé;
- Suite à un incident, un post-mortem devrait toujours être fait, suivi de la rédaction d'un rapport;
- Un registre contenant une liste et une réserve de ressources essentielles et adéquatement formées doit être constitué. Le registre doit être actualisé et intégré au plan d'urgence;

[57] Tiré de Bernier, Beaudry, société d'avocats, Institut International de recherche, décembre 2000.

- Les partenaires doivent aussi avoir leur plan de sécurité, satisfaire aux mêmes exigences et être audités;
- Les plans d'urgence doivent tenir compte des autres impératifs de sécurité tels la confidentialité, l'intégrité des données et la disponibilité (informations, systèmes).

Gestion des changements

La gestion des changements est plus générale que la sécurité. Il est par contre très important de considérer et d'intégrer les éléments de sécurité dans la gestion même des changements (ex: gestion des configurations, etc...). De plus, les changements apportés aux mécanismes de sécurité doivent être gérés de façon adéquate.

2.4.4 Dimension technologique

Lorsqu'il est question de sécurité de l'information numérique et des échanges électroniques, la dimension technologique est certainement celle dont on discourt le plus facilement. Les thématiques qui sont généralement abordées ont trait aux fonctions (appelées dans certains cas services) de sécurité, de même qu'aux mécanismes de sécurité et solutions technologiques qui supportent ces fonctions. Tel que nous le verrons plus en détails à la section 2.5, les mécanismes de sécurité et solutions technologiques déployés doivent supporter les fonctions suivantes :

- Intégrité ;
- Irrévocabilité ;
- Identification/authentification ;
- Habilitation/contrôle d'accès ;
- Confidentialité ;
- Disponibilité ;
- Surveillance ;
- Administration.

Plusieurs considèrent qu'on obtient le meilleur niveau de sécurité en sélectionnant et en déployant les meilleurs mécanismes de sécurité et solutions technologiques. Un sondage informel réalisé par Gartner auprès d'utilisateurs de solutions technologiques révèle d'ailleurs que leur première action lorsqu'ils visent à corriger une vulnérabilité ou à répondre à un incident de sécurité est d'identifier et d'acheter un bon produit de sécurité[58].

Cette vision fort répandue fait abstraction des nombreux éléments juridiques, organisationnels et humains que nous avons abordés dans les sections précédentes mais aussi d'éléments technologiques moins communément considérés mais tout aussi importants que le déploiement de mécanismes de sécurité et solutions technologiques. Parmi ces éléments, notons les activités suivantes dans lesquelles la sécurité doit être considérée :

[58] W. Malik, *Do Security Products Alone Solve the Problem ?*, Gartner Group, 16 Janvier 2001

- le développement, l'entretien et la mise à jour des applications (de sécurité ou autre) ;
- la sélection des applications ou équipements ;
- l'installation et la paramétrisation des applications ou équipements (de sécurité ou autre).

Le simple déploiement de mécanismes de sécurité et solutions technologiques ne peut pallier aux brèches de sécurité et aux vulnérabilités qu'ont peut retrouver au cœur même des systèmes d'exploitation, applications ou équipements qui auraient été mal conçus, développés, sélectionnés, installés ou configurés. Dans un tel contexte, le déploiement de mécanismes de sécurité et de solutions technologiques tels que ceux présentés à la section 2.5 ne constituerait qu'un « cataplasme sur une jambe de bois ». Plutôt que de tenter de pénétrer en force dans un système, en brisant un algorithme de chiffrement par exemple, les « hackers » utilisent souvent ces failles pour pénétrer dans un système et s'approprier les informations.

Les responsables des activités de développement, de sélection, d'installation et de paramétrisation de produits doivent donc inclure la sécurité parmi les éléments à considérer tout au long de celles-ci. Les sections suivantes décrivent certains points à considérer pour chacune de ces activités. Ces éléments devraient être inclus dans le cadre de gestion de la sécurité.

2.4.4.1 Développement, entretien et mise à jour des applications

Le processus de développement constitue le point de départ de la vie des applications. Une application mal conçue et programmée peut abriter des failles qui mettront en péril l'intégrité, la confidentialité et la disponibilité des informations numériques qu'elle contient, qu'elle gère ou qui transitent par elle. Ceci concerne autant les applications de sécurité que les applications d'entreprises. À titre d'exemples, considérons les situations suivantes :

- Une base de données est conçue sans qu'on y intègre une fonction « commit/roll-back » permettant de garantir l'intégrité des informations numériques si une transaction est stoppée en cours de route. On ne peut donc pas garantir l'intégrité des informations numériques à l'intérieur de la base de données.
- Un répertoire contenant les clés publiques de chiffrement n'a pas été testé pour vérifier sa robustesse et est souvent hors service. Les applications utilisant ce répertoire pour offrir notamment la fonction d'identification/authentification ne pourront assurer cette dernière.

Les points suivants doivent donc être considérés lors du processus de développement des applications ainsi que lors de l'entretien et de la mise à jour des applications afin de garantir l'intégrité, la confidentialité et la disponibilité des données :

- **Conception tenant compte des notions de sécurité**. À la base, l'application doit être conçue de façon à minimiser les lacunes et les brèches de sécurité et à assurer l'intégrité, la confidentialité et la disponibilité des informations numériques qu'elle contient ou gère.

- **Utilisation de langages de programmation et d'interfaces de programmation d'applications (API) garantissant une certaine sécurité**. Les langages de programmation robustes qui offrent des fonctions de vérification du code et d'authentification du code devraient être privilégiés. De plus, comme aucun langage n'est entièrement sécuritaire, les programmeurs devraient connaître les lacunes de sécurité de ces langages, de même que les solutions de contournement. Plusieurs livres et références Internet traitent de ces thèmes.

- **Revues de code incluant des critères de sécurité**. Le cycle de développement devrait inclure des revues de code permettant entre autres de s'assurer que le code ne contient aucune lacune de sécurité. Ces revues de code doivent être effectuées par des programmeurs bien au fait des lacunes de sécurité du langage employé et des solutions de contournement.

- **Cycle de développement impliquant différentes phases d'essais**. Le cycle de développement d'applications devrait inclure des phases d'essais permettant de tester le code (essais unitaires) et les fonctionnalités dans un environnement d'exploitation (essais intégrés et de pré-production) ou non (essais fonctionnels). Ces essais permettent entre autres de tester si l'application assure l'intégrité, la confidentialité et la disponibilité des données.

  Afin de valider la sécurité des applications, il est recommandé d'utiliser certains critères d'évaluation spécifiques à cette tâche. Ces critères peuvent être développés sur mesure mais peuvent aussi s'inspirer de critères existants tels que les « Critères communs ». Les « Critères communs », qui font l'objet d'une normalisation à l'échelle internationale (ISO/IEC 15408), définissent un ensemble d'exigences, dont la validité est connue, et qui peuvent être utilisées pour établir les exigences de sécurité de futurs produits et systèmes. Ils définissent aussi la structure des profils de protection qui permettent aux utilisateurs et aux développeurs potentiels de créer des ensembles normalisés d'exigences de sécurité pour répondre à leurs besoins[59].

- **Essai des systèmes développés dans un contexte reproduisant le contexte d'utilisation réel**. Les différents essais dont il est question dans le point précédent ne tiennent pas compte des interactions pouvant exister entre les différents produits installés dans un même environnement. Ces interactions peuvent avoir un effet négatif sur la sécurité des applications et équipements. Si c'est le cas, ces effets doivent être observés et documentés et des solutions doivent être développées.

- **Mise en place d'un environnement de graduation/rétrograduation (incluant versionnage)**. Un bon environnement de graduation/rétrograduation doit être mis en place afin d'éviter de perdre le contrôle des sources (code) et ainsi éviter leur perte d'intégrité.

- **Environnement de développement sécurisé de façon à éviter les intrusions et la manipulation du code**. L'environnement de développement doit être isolé et uniquement accessible par des personnes dûment autorisées. Les postes de développement branchés à l'environnement de développement doivent être configurés de façon à ne pas constituer une menace envers ce dernier. Ceci est particulièrement vrai des postes branchés à Internet et des postes à distance.

- **Utilisation de modules ou d'objets éprouvés à l'intérieur d'un projet de développement**. Lorsque possible, on préférera utiliser des modules ou objets ayant été testés et éprouvés plutôt que de les développer sur mesure. Attention aux scripts utilisés dans le monde Internet, car ceux-ci constituent une menace importante puisqu'ils sont rarement bien conçus. Pour les mêmes raisons, on doit faire attention aux divers modules gratuits que l'on retrouve sur Internet.

[59] On se référera à la norme ISO/IEC 15408 ou aux documents *Critères communs pour l'évaluation de la sécurité des TI* et *Méthodologie commune pour l'évaluation de la sécurité des TI* pour plus d'informations.

2.4.4.2 Sélection des applications et équipements

Les fournisseurs d'applications et d'équipements ne sont pas non plus à l'abri de failles issues des étapes de développement des produits. L'acheteur de ces solutions doit donc s'assurer que ces produits comptent peu de failles de sécurité ou que celles-ci sont à tout le moins connues et qu'il existe des solutions pour les corriger.

Les points suivants doivent donc être considérés lors du processus de sélection des applications et des équipements de l'infrastructure afin de garantir que ceux-ci sont sécuritaires :

- **Réalisation d'une analyse des produits**. Les technologies de l'information sont soumises à une panoplie d'essais et de comparaisons de la part des médias spécialisés et des firmes d'analystes. Dans plusieurs cas, des critères de sécurité sont utilisés pour juger de la qualité du produit. Une étude détaillée de ces différents rapports d'analyse devrait être réalisée.

- **Évaluation des produits à l'aide de critères standards d'évaluation de la sécurité.** Comme c'est le cas lors du développement d'applications, il est recommandé d'utiliser certains critères spécifiques à l'évaluation de la sécurité lors de l'acquisition d'applications et d'équipements. On utilisera directement des critères déjà établis tels que les « Critères communs » ou on développera ses propres critères en se basant sur ceux-ci. On doit souligner l'avantage d'avoir recours à des critères tels que les « Critères communs » (ou norme ISO/IEC 15408) ou les critères ITSEC (Europe),TCSEC (États-Unis) et CTCPEC (Canada)[60]. En effet, ces critères et la certification qui y est attachée[61], sont reconnus mondialement par les fournisseurs de solutions et leurs grands clients. Plusieurs produits commerciaux et systèmes propriétaires ont d'ailleurs déjà été évalués et certifiés à l'aide de ces critères par des centres d'évaluation gouvernementaux et commerciaux situés un peu partout à travers le monde. Lorsque nécessaire, une homologation de produits pourrait s'effectuer selon la même approche.

- **Essai des produits dans un contexte reproduisant le contexte d'utilisation réel**. Les deux points précédents ne tiennent pas compte des interactions pouvant exister entre les différents produits installés dans un même environnement. Ces interactions peuvent avoir un effet négatif sur la sécurité des applications et équipements. Si c'est le cas, ces effets doivent être observés et documentés et des solutions doivent être développées.

2.4.4.3 Installation et paramétrisation des applications ou équipements

Une mauvaise installation ou paramétrisation des applications ou des équipements de l'infrastructure peut créer des brèches de sécurité, peu importe le niveau de sécurité de ceux-ci. À titre d'exemples, considérons les situations suivantes :

- Un coupe-feu de bonne qualité ayant une certification « Critères communs » (ou ISO/IEC 15408) de niveau EAL4 (plus haut niveau obtenu pour un coupe-feu jusqu'à maintenant) est installé. Celui-ci est

[60] Les critères ITSEC, TCSEC et CTCPEC sont toujours utilisés mais sont graduellement remplacés par les « Critères communs » (ou la norme ISO/IEC 15408)

[61] La certification « Critères communs » compte sept niveaux de certification, soit : EAL1 – testé fonctionnellement, EAL2 – testé structurellement, EAL3 – testé et vérifié méthodiquement, EAL4 – conçu, testé et vérifié méthodiquement, EAL5 – conçu et testé de façon semi-formelle, EAL6 – vérifié, conçu et testé de façon semi-formelle, EAL7 – vérifié, conçu et testé de façon formelle.

mal configuré lors de son installation et laisse entrer des paquets de données qu'il ne devrait normalement pas laisser entrer. Le contrôle d'accès se réalisant mal, la confidentialité et l'intégrité des données ne sont plus nécessairement garanties.

- Plusieurs mécanismes de sécurité sont installés et configurés correctement. Cependant, les mises à jour de sécurité du système d'exploitation et des fureteurs des employés n'ont pas été faites depuis longtemps. Ceux-ci représentent une faiblesse que les meilleurs mécanismes de sécurité ne peuvent compenser.

Les points suivants doivent donc être considérés lors du processus de sélection des applications et équipements afin de garantir que ceux-ci sont sécuritaires :

- **Installation et paramétrisation des applications ou équipements**. Les applications et équipements devraient être installés et configurés par des individus compétents et selon les instructions du fournisseur. Les responsables de ces activités devraient s'assurer de consulter les informations mises à jour par les fournisseurs à cet effet et demander l'aide de ces derniers lorsque nécessaire. Les modifications ultérieures à la paramétrisation devraient aussi être effectuées selon les instructions du fournisseur par un individu compétent.

- **Mise à jour des systèmes d'exploitation et applications**. Il ne se passe généralement pas une journée sans que les fournisseurs ou la communauté des experts en sécurité ne mettent à jour une faille dans les systèmes d'exploitation et applications commerciales. À titre d'exemple, le numéro du 7 mai 2001 de la publication « CyberNotes » du FBI recense 47 vulnérabilités découvertes dans des applications commerciales, et ce uniquement entre le 6 avril et le 3 mai. Il est donc essentiel qu'une surveillance continuelle s'effectue et que les correctifs et mises à jour soit appliqués au besoin.

- **Configuration des postes de travail**. La configuration des postes de travail est un élément extrêmement délicat qui suscite des débats presque idéologiques. D'un côté, certains recommandent d'exercer un contrôle absolu des postes de travail, de n'y installer que les applications approuvées et de les isoler de l'Internet, de l'autre, les partisans de l'individualisme qui laissent le contrôle des postes de travail au bon gré des utilisateurs. L'expert en sécurité aura tendance à recommander la première option puisqu'elle est celle qui garantit davantage la sécurité des postes de travail. Cependant, la réalité humaine et organisationnelle est telle qu'un compromis est généralement nécessaire.

  Dans ce contexte, certains éléments de sécurité doivent être considérés dans la configuration d'un poste de travail :

  - Partage de fichiers et d'imprimantes : cette option devrait être désactivée. Les fichiers devraient être partagés à l'aide de répertoires sur le réseau.
  - Détecteur de virus : un détecteur de virus devrait être déployé sur chaque poste de travail.
  - Messagerie instantanée (ICQ, MSN Messenger, etc.) : ces logiciels créent des failles de sécurité et devraient être proscrits.
  - Outils de recherche et de partage de fichiers (Napster, Hotline, Gnutella). Ces logiciels créent des failles de sécurité et devraient être proscrits.
  - Coupe-feu personnel : un coupe-feu personnel devrait être installé sur tout poste de travail qui se branche à distance à partir d'un modem câble ou LNPA.

- Mises à jour de sécurité : les mises à jour de sécurité devraient être faites aussi sur les postes de travail.

La sécurité des postes dépend donc d'un certain nombre de facteurs internes et externes à l'organisation. Les décisions relatives à la sécurité des postes devraient donc reposer sur certaines exigences de base adaptées au contexte spécifique d'utilisation.

2.5 Les fonctions et composantes de sécurité logiques

Cette section présente l'ensemble des fonctions de sécurité[62] de l'information numérique, de même que les mécanismes et solutions technologiques s'y rattachant. Bien qu'on les relie souvent à la dimension technologique, le présent document présentent ces composantes dans une section séparée étant donné que certaines composantes ont un fort impact sur d'autres dimensions de la sécurité.

Tel que spécifié précédemment, le choix de ces fonctions, mécanismes de sécurité et solutions technologiques se base sur l'étude approfondie des normes internationales (ISO/IEC 10181, ISO/IEC 13335 et ISO 7498-2)[63] et de certains projets d'architecture gouvernementale de sécurité effectués dans les dernières années aux États-Unis et en Europe.

Plus spécifiquement, le découpage des fonctions de sécurité s'inspire largement de la norme ISO/IEC 10181 qui établit un cadre permettant de spécifier les fonctions de sécurité pour les systèmes ouverts. La norme ISO/IEC 13335, qui se veut un guide pour la gestion de la sécurité des technologies de l'information, a été utilisée afin de raffiner le découpage et d'adresser les fonctions de surveillance et d'administration. Cette norme sert également de base au Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise[64].

Les fonctions suivantes ont été retenues dans le cadre de l'AGSIN :

- Fonction d'intégrité ;
- Fonction d'irrévocabilité ;
- Fonction d'identification/authentification ;
- Fonction d'habilitation/contrôle d'accès ;
- Fonction de confidentialité ;
- Fonction de disponibilité ;
- Fonction de surveillance ;
- Fonction d'administration.

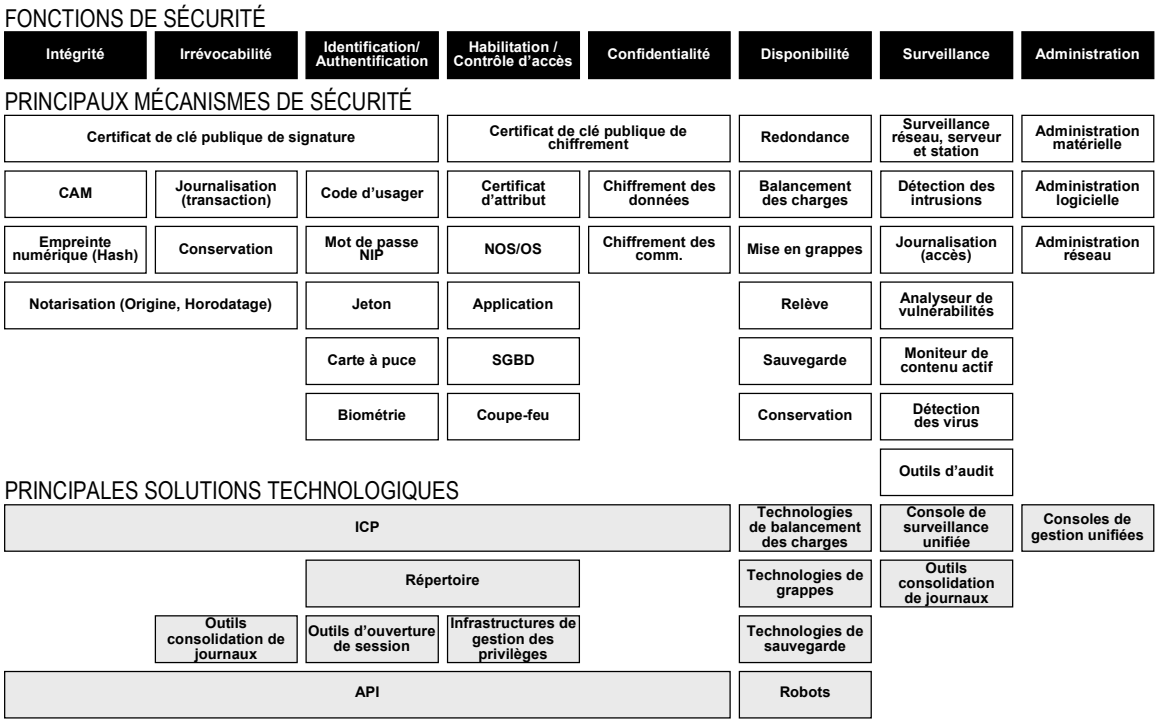
Comme le démontre la figure suivante[65], chacune de ces fonctions peut être supportée par différents mécanismes de sécurité et solutions technologiques. Les mécanismes sont des processus, logiciels ou

[62] Fonction de sécurité (inspirée de la norme ISO 7498-2) : Fonction, fournie par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données.
[63] On se référera à l'annexe D et aux normes ISO/IEC 10181 et ISO 7498-2 pour plus de détails.
[64] On se référera au *Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise* (février 2001) basé sur la norme ISO/IEC 13335 produit par le SCT pour plus d'informations.
[65] Les acronymes contenus dans la figure sont définis à l'annexe B.

équipements technologiques ayant pour but justement de remplir les diverses fonctions de sécurité. De leur côté, les solutions technologiques sont des ensembles de solutions permettant la gestion des différents mécanismes proposés.

Selon la firme Gartner, « l'énoncé des différentes fonctions de sécurité [de l'AGSIN] rencontre les meilleures pratique du marché et la catégorisation en vigueur »[66].

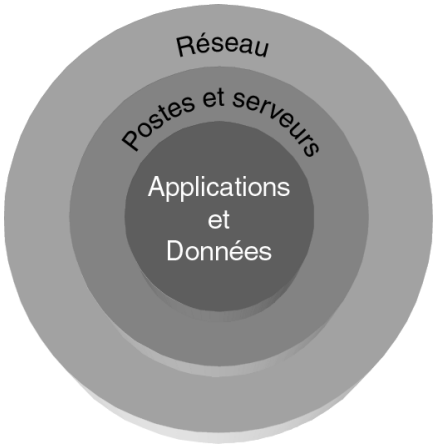
FONCTIONS DE SÉCURITÉ, PRINCIPAUX MÉCANISMES DE SÉCURITÉ ET PRINCIPALES SOLUTIONS TECHNOLOGIQUES[67]



Comme le démontre la figure suivante, l'ensemble de ces mécanismes de sécurité et solutions technologiques visent autant la protection des réseaux (périmètres) que celle des postes de travail, serveurs, applications et informations (données). Cette façon d'aborder les choses correspond aux nouvelles exigences générées par les affaires électroniques. En effet, si la protection du périmètre à l'aide de mécanismes de sécurité tels que les coupe-feu s'avérait le moyen de défense privilégié dans les premières années de l'Internet, elle est maintenant insuffisante pour assurer la protection complète et efficace d'une organisation se livrant à des échanges électroniques. Ainsi que nous le verrons dans les prochaines sections, de nouvelles catégories de mécanismes de sécurité et de solutions technologiques sont nécessaires pour réaliser cet objectif.

[66] On se référera au document *Commentaires sur le troisième bien livrable produit par CGI, Gartner Consulting* pour plus de détails.
[67] Certaines composantes telle que l'ICP ont un très fort impact organisationnel.

ÉTENDUE DE LA SÉCURITÉ



Les différentes fonctions de sécurité sont présentées plus en détails dans les sections suivantes. Les éléments suivants sont traités dans chacune de ces sections :

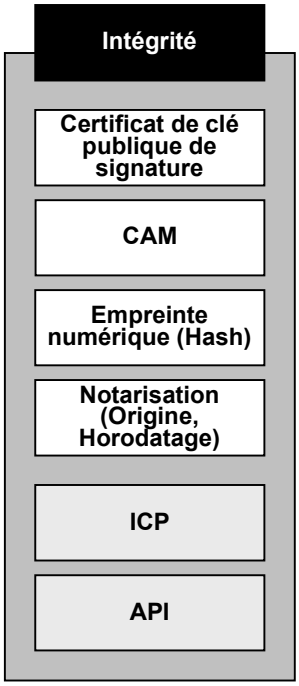
- Description de la fonction ;
- Tendances du marché ;
- Règles architecturales[68] ;
- Normes et standards.

Notons trois points facilitant la lecture de ces différentes sections :

- la définition des différents mécanismes de sécurité et solutions technologiques est présentée à l'annexe B de ce document. La description des différentes normes et standards est présentée à l'annexe D;
- les différentes règles architecturales sont accompagnées d'une lettre (ou de plusieurs) entre parenthèses. Celle-ci fait référence au niveau de sécurité auquel s'applique cette exigence, tel que défini dans le « Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité » du SCT. « B » indique un bas niveau de sécurité, « M » indique un niveau de sécurité moyen, « É » indique un niveau de sécurité élevé et « G » indique tous les niveaux de sécurité à la fois;
- les normes et standards en caractères gras sont des normes et standards particulièrement dominants qui doivent (si nécessaire) être considérés dans l'élaboration d'une architecture de sécurité de l'information numérique.

[68] Une règle architecturale vise à définir à un niveau de détail plus précis, les règles applicables à chacune des fonctions de sécurité. Elle oriente la conduite des travaux et porte sur les éléments à considérer lors de l'élaboration d'une architecture détaillée de sécurité.

2.5.1 Fonction d'intégrité



Description

La fonction d'intégrité est responsable d'assurer qu'une information n'a pas été modifiée ou détruite sans autorisation de façon volontaire ou accidentelle, et ce, si nécessaire, tout au long du cycle de vie de l'information.

Cette fonction est supportée par les mécanismes de sécurité et solutions technologiques suivants : certificat de clé publique de signature, code d'authentification de message (CAM), empreinte numérique, notarisation (horodatage), infrastructure à clés publiques (ICP) et interface de programmation d'applications (API).

Tendances de l'industrie

- Dans le contexte des échanges électroniques, la fonction d'intégrité vise à ce que l'information numérique soit reçue dans les mêmes conditions qu'elle a été émise. Elle constitue une protection contre la falsification non détectée des informations en transit. Pour obtenir ce résultat, une valeur de vérification d'intégrité (CAM, bit de parité, somme de contrôle, empreinte numérique) est habituellement ajoutée à l'information numérique (message, transaction, etc.), à proximité de l'indication de sa source. Le récepteur possède une clé privée lui permettant de recalculer la valeur de vérification d'intégrité et donc de vérifier si celle qu'il a reçue est correcte. Cette valeur se calcule comme une fonction mathématique, avec la particularité que toute modification apportée à l'information numérique ou à cette valeur par un attaquant a une forte probabilité de produire une vérification d'intégrité discordante.
- Les logiciels de détection de virus utilisent habituellement aussi une somme de contrôle pour tout fichier dans le système et l'enregistrement de ces sommes de contrôle dans un endroit sûr. Cette procédure de contrôle vérifie ensuite l'intégrité des fichiers en recalculant à intervalle régulier toutes ces sommes de contrôle et en les comparant avec celles enregistrées. Si l'une des sommes de contrôle diffère, cela peut indiquer une infection possible de ce fichier par un virus.
- La messagerie électronique conventionnelle (MIME ou SMTP) ne garantissant pas l'intégrité des messages, entre autres choses, des efforts importants ont été investis dans les dernières années afin de développer des protocoles qui offrent cette fonction. S/MIME, X.400 et « Privacy-Enhanced Mail » (PEM) sont des exemples de protocoles qui visent à garantir l'intégrité des messages. Les produits supportant la norme S/MIME tels que Microsoft Outlook, Lotus Notes et Netscape Navigator sont massivement adoptés comme outils de messagerie électronique. Cependant l'adoption du standard S/MIME par les organisations se fait attendre puisqu'il présente certaines problématiques telles que la

gestion des clés de chiffrement ou le manque de compréhension des mécanismes par les utilisateurs potentiels.

- L'utilisation d'un mécanisme de notarisation basé sur le concept de tierce partie de confiance est de plus en plus promue pour garantir l'intégrité des données.

Règles architecturales

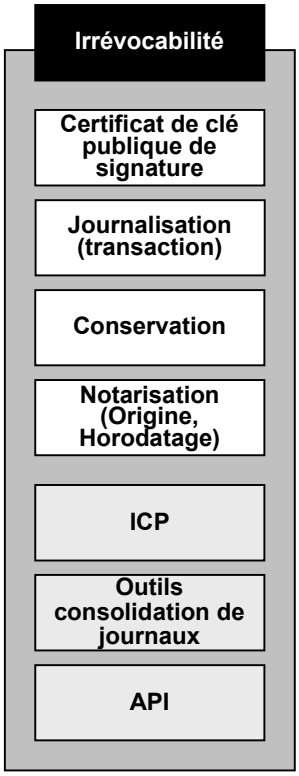
- **Appliquer un plan d'intégrité des données lié à la nature de l'information numérique et au contexte (G)** (par exemple bit de parité, total de contrôle, CAM, empreinte numérique, horodatage, signature numérique, etc.).

Normes et standards

- ISO/IEC 10181-6
- ISO/IEC 9797
- ISO/IEC 10118
- FIPS PUB 180-1

De plus, la plupart des standards touchant le stockage des informations numériques, les échanges électroniques et les certificats ont comme but de garantir l'intégrité des données. À titre d'exemple, notons X.509, IPSec, S/MIME, PEM, IETF RFC 2402 (« IP Authentication Header »), IETF RFC 2406, (« IP Encapsulating Security Payload »), ISO/IEC 11577 (« Open Systems Interconnection -- Network layer security protocol ») et IEEE 802.10 (« Local and Metropolitan Area Networks (MANs): Interoperable LAN/MAN Security (SILS) »).

2.5.2 Fonction d'irrévocabilité



Description

La fonction d'irrévocabilité assure qu'une action ou qu'un document est indéniable et clairement attribué à l'entité qui l'a généré et ce, tout au long du cycle de vie de l'information si nécessaire.

Selon la norme ISO 13888 (Technologies de l'information - Techniques de sécurité - Non-répudiation), il existe quatre types d'irrévocabilité, soit :

- *Irrévocabilité d'origine* visant la protection contre toute tentative de l'expéditeur de nier le fait qu'il a envoyé les données.
- *Irrévocabilité de réception* visant la protection contre toute tentative du destinataire de nier le fait d'avoir reçu les données.
- *Irrévocabilité de dépôt* visant à fournir l'évidence que l'expéditeur a bel et bien envoyé les données à une tierce partie de confiance
- *Irrévocabilité de livraison* visant à fournir l'évidence que les données ont été livrées au destinataire par la tierce partie de confiance

Cette fonction est supportée par les mécanismes de sécurité et solutions technologiques suivants : certificat de clé publique de signature, journalisation des transactions, conservation, notarisation, infrastructure à clés publiques (ICP), outils de consolidation des journaux et interface de programmation d'applications (API).

Tendances de l'industrie

- La journalisation des transactions a longtemps constitué un des seuls éléments de preuve permettant de rendre compte des actions des individus. Cependant, ce mécanisme possède plusieurs désavantages dont le fait d'être une preuve insuffisante si prise individuellement (l'individu au bout du clavier peut ne pas être le bon) ou la nécessité d'effectuer la tâche fastidieuse de l'analyse des journaux. Des outils de consolidation permettent d'automatiser davantage cette tâche depuis quelques années.
- La signature d'un message en chiffrant la valeur de vérification d'intégrité d'un paquet de données ou d'un message avec une clé privée connue du seul émetteur, est une méthode d'obtention de l'irrévocabilité dont on fait de plus en plus usage. Si le message contient une date et une heure (horodatage) et si le destinataire vérifie le moment d'arrivée et garde une copie signée du message, le récepteur possède une irrévocabilité avec preuve d'origine.
- L'utilisation d'un mécanisme de notarisation basé sur le concept de tierce partie de confiance est de plus en plus promu pour assurer l'irrévocabilité. En plus d'être utilisée pour garantir de l'intégrité des informations numériques, la notarisation est utilisée pour garantir certaines propriétés relatives aux informations échangées entre deux entités, telles que leur origine ou l'heure à laquelle elles ont été envoyées ou reçues.

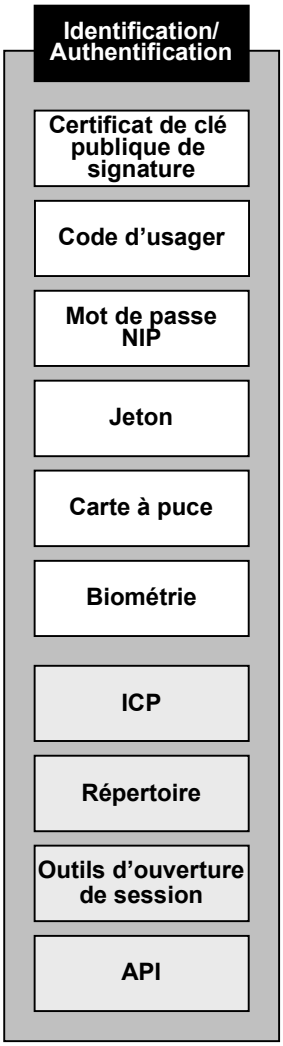
Règles architecturales

- **Offrir des applications ou commandes permettant aux utilisateurs de chiffrer/déchiffrer facilement des données, d'y apposer une signature numérique et de la vérifier (M,É)**.
- **Conserver au niveau des applications des informations relatives aux échanges électroniques** (transactions, transferts de fichiers, etc.) **(G)**.

Normes et standards

- ISO/IEC 10181-4
- ISO/IEC 13888

2.5.3 Fonction d'identification/authentification



Description

La fonction d'identification permet d'identifier une entité (personne ou autre) ou encore de répondre à la question « Qui est cette entité? ». L'authentification sert à authentifier une entité ou encore à répondre à la question « Cette entité est-elle celle qu'elle dit être? ». Si nécessaire, cette fonction peut être applicable tout au long du cycle de vie de l'information.

Cette fonction inclut les mécanismes de sécurité et solutions technologiques suivants :

Authentification forte : certificat de clé publique de signature, jeton, carte à puce, mécanismes biométriques, infrastructure à clés publiques (ICP), outils d'ouverture de session (accès simplifié) et répertoire.

Authentification faible : code d'usager, mot de passe, numéro d'identification personnelle (NIP).

Une interface de programmation d'applications (API) supporte aussi la fonction d'identification/authentification.

Tendances de l'industrie

- Le mécanisme d'identification/authentification par code d'usager et mot de passe est le plus répandu et n'est pas voué à disparaître à courte échéance puisqu'il constitue la méthode la plus facile à utiliser et à mettre en œuvre, en plus d'être très peu coûteuse. On continuera de l'utiliser lorsque le niveau de risque est faible.
- Les mécanismes d'identification/authentification sont souvent combinés afin de garantir un niveau de sécurité plus élevé. Ainsi, le certificat de signature est généralement combiné à un mot de passe et peut être combiné à une carte à puce ou à des systèmes biométriques.
- À l'échelle mondiale, le nombre de projets d'ICP en opération est relativement faible, bien que de nombreux projets pilotes aient été entrepris. IDC prévoit cependant que dans les prochaines années, la croissance du marché des ICP et des certificats sera graduelle et que le nombre d'ICP en production augmentera sensiblement.
- Les certificats sont particulièrement utilisés dans les applications entreprise à entreprise.
- La majorité des projets d'authentification à l'aide de certificats utilisent des certificats obéissant à la norme X.509 de l'UIT (L'annuaire: cadre d'authentification), font appel à des répertoires de la norme X.500 de l'UIT (L'Annuaire: Vue d'ensemble des concepts, modèles et services) ou à des répertoires compatibles à LDAP et utilisent le protocole d'accès LDAP.
- Au niveau de l'authentification des serveurs, l'utilisation de certificats SSL Serveur est la pratique la plus courante.
- L'approche de « roaming » qui favorise la portabilité en permettant de stocker les certificats dans une base de données éloignée et d'y accéder à l'aide d'une autre méthode d'authentification (un code d'utilisateur/mot de passe ou un jeton par exemple) est une approche montante de plus en plus populaire. Elle peut remplacer l'utilisation conjuguée d'une carte à puce et d'un certificat de signature.
- La majorité des fournisseurs de solutions de répertoires ont délaissé le standard X.500 ou recentré leurs efforts de développement et de marketing sur des solutions LDAP.
- En Amérique, outre son utilisation bien connue dans le domaine de la téléphonie où elle agit plus à titre de porte-monnaie électronique, la carte à puce fait une avancée subtile dans le secteur financier et bancaire en particulier. Le marché nord-américain accuse cependant un retard extrêmement important par rapport à l'Europe où la carte à puce est utilisée dans plusieurs secteurs (financier, santé, télécommunication, etc.) depuis une vingtaine d'année.
- Les jetons sont utilisés principalement pour permettre l'authentification forte d'employés lors d'accès à distance. Ils sont aussi utilisés, mais de façon moins courante, pour restreindre l'accès à des systèmes à des employés, à des clients ou fournisseurs importants (par exemples, sites Web ou systèmes de commande).
- Les jetons utilisant le port USB sont un concurrent de plus en plus important à la carte à puce et aux jetons traditionnels (logiciel ou matériel).
- Considérant ses coûts d'implantation, sa complexité et sa faible acceptabilité sociale, la biométrie est relativement peu utilisée, particulièrement dans les applications civiles.
- La reconnaissance de l'empreinte digitale est, et sera sans conteste, la technologie biométrique dominante, suivie de loin par les autres technologies.

- En offrant des mécanismes d'ICP, de répertoire et de support des cartes à puce directement dans Windows 2000, Microsoft fera fort probablement une avancée importante dans les entreprises au niveau de la sécurité de l'information.

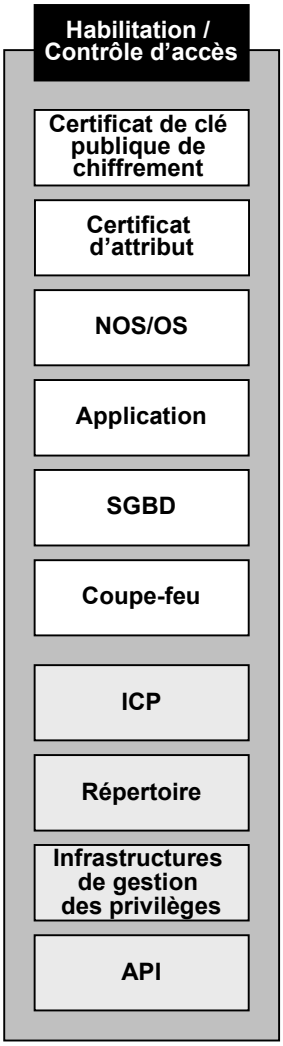
Règles architecturales

- **Utiliser le mécanisme d'authentification approprié à la valeur des informations numériques et/ou échanges électroniques (G)**. Tel qu'on peut le voir dans le tableau « Mécanismes de sécurité et solutions technologiques à utiliser selon le niveau de sécurité » à la section 2.6.1, certains mécanismes d'identification/authentification sont plus appropriés dans le cas où les informations sont de basse valeur alors que d'autres sont plus appropriés dans le cas où les informations sont de valeur élevée.
- **Utiliser le mécanisme d'authentification approprié au type d'activité ou échange (G)**. Les différents mécanismes d'authentification ne sont pas appropriés à toutes les situations. Giga Information Group recommande par exemple d'utiliser le certificat numérique principalement pour l'accès à des systèmes à accès restreint, l'accès à haute fréquence à des sites Web sécurisé et l'authentification des parties habilitées, par exemple les places d'affaires virtuelles. Le jeton est particulièrement approprié pour l'accès à distance. La carte à puce est davantage recommandée pour l'accès à distance, la réalisation et le paiement de commande de haute valeur. La biométrie est quant à elle particulièrement recommandée pour l'accès aux installations ou aux ordinateurs et l'accès à distance.
- **Utiliser des méthodes d'authentification à multiples mécanismes (M et É)**. La combinaison de plusieurs mécanismes d'authentification permet généralement d'atteindre des niveaux de sécurité encore plus élevés. Les experts recommandent de combiner un ou plusieurs des mécanismes suivants : « Ce qu'une personne sait » (un mot de passe, la réponse à une question, etc.), « ce qu'une personne possède » (un certificat, un jeton d'authentification, une carte à puce, etc.), « ce qu'une personne est » (biométrie) et « où se trouve une personne » (numéro de téléphone, adresse IP, etc.).
- **Utiliser des certificats SSL afin d'authentifier les serveurs et s'assurer qu'ils sont à jour (M)**. Ces certificats permettent non seulement de chiffrer les données, mais aussi d'authentifier les serveurs, ce qui joue un rôle important dans la confiance des utilisateurs.
- **Lorsqu'une authentification est nécessaire, chaque utilisateur doit posséder son propre élément d'authentification (G)**. Ceci permet une meilleure traçabilité. L'utilisation d'un élément d'authentification générique (mot de passe ou autres) est à proscrire à moins que l'individu se soit déjà authentifié à l'aide d'un élément d'authentification.
- **Ne pas utiliser des certificats qui ont été émis après une simple vérification de l'adresse de courrier électronique (M et É)**. Ce type de certificat n'est absolument pas admissible aux fins d'authentification. L'utilisation d'un mot de passe fournit un niveau de sécurité plus important.
- **Avoir recours à des règles de création de mots de passe sécuritaires (G)** si un mécanisme d'authentification par mot de passe non-dynamique est utilisé. Les règles décrites dans le standard FIPS PUB 112 sont des exemples de règles à suivre.
- **Protéger l'envoi des mots de passe contre l'interception en utilisant un protocole de transformation des mots de passe (B et M)**. S/Key et Kerberos par exemple permettent de traiter un mot de passe non-dynamique à l'aide d'une fonction « à sens unique » de façon à créer un mot de passe transformé. Ce mot de passe transformé est différent à chaque fois qu'il est envoyé. Comme les mots de passe sont traités à l'aide d'une fonction à sens unique, ils ne peuvent être reconstitués par des « oreilles indiscrètes ».

Normes et standards

- ISO/IEC 10181-2
- ISO/IEC 7816
- HA-API
- IEEE P1363
- **PKCS de RSA**
- **PKIX de l'IETF**
- **X.509 de l'UIT**
- SPKI de l'IETF
- **Certificat WTLS du WAP Forum**
- XML Signature du W3C
- S2ML
- XKMS
- Kerberos
- **X.500 de l'UIT**
- DAP
- **LDAP**
- **FIPS PUB 112**

2.5.4 Fonction d'habilitation/contrôle d'accès



Description

La fonction d'habilitation/contrôle d'accès (« Que m'est-il permis de faire ») définit une liste de ressources et d'informations auxquelles une entité (personne ou autre) peut accéder une fois qu'elle a été dûment authentifiée. Les mécanismes de contrôle de l'accès permettent notamment aux systèmes de contrôler exactement à qui le droit d'accès est accordé, pour quelles ressources et de quelle façon, les autorisation à poser des gestes et à modifier des données, etc. Si nécessaire, cette fonction peut être applicable tout au long du cycle de vie de l'information.

Cette fonction contient les mécanismes de sécurité et solutions technologiques suivants : certificat de clé publique de chiffrement, certificat d'attribut, mécanismes d'habilitation des systèmes d'exploitation (NOS/OS), des applications et des systèmes de gestion de bases de données (SGBD), accès à distance, coupe-feu, infrastructure à clés publiques (ICP), infrastructures de gestion des privilèges et répertoire et interface de programmation d'applications (API)

Tendances de l'industrie

- Malgré leur faible niveau de sécurité, les principaux contrôles d'accès aux réseaux et aux ordinateurs à l'intérieur des organisations passent par les systèmes d'exploitation.
- Les mécanismes de gestion des accès inclus dans les applications et bases de données sont, et de loin, les mécanismes de contrôle d'accès aux applications les plus utilisés dans l'industrie. Ils sont à quelques exceptions près toujours utilisés en collaboration avec un mécanisme d'identification/authentification par code d'utilisateur/mot de passe.
- Le recours aux coupe-feu pour protéger les réseaux internes des tentatives d'intrusion issues des réseaux publics est de pratique courante dans l'industrie et les gouvernements.
- La technologie de coupe-feu la plus répandue dans les organisations et gouvernements est la technologie de type filtrage de paquets (de données), bien que celle-ci soit beaucoup moins efficace et performante que la technologie « Stateful inspection » ou que la technologie de passerelle applicative (« application proxy »).

- Les organisations possédant des infrastructures importantes adoptent des coupe-feu dédiés. Plutôt que d'utiliser un produit « tout-en-un », on choisit plutôt d'ajouter au coupe-feu dédié des options permettant la réalisation de RPV et on utilisera des produits de tierces parties pour la détection des virus, le monitorage et autres.
- En plus de leur principale utilisation consistant à contrôler les accès à un réseau, les coupe-feu peuvent être utilisés pour la création de zones démilitarisées permettant de séparer des serveurs ayant des similarités. On peut par exemple créer une zone contenant des serveurs Web, une autre contenant des serveurs transactionnels et une troisième contenant des serveurs de bases de données.
- Les infrastructures de gestion des privilèges tels que Site Minder de Netegrity ou getAccess de Entrust sont des outils fort prometteurs et de plus en plus utilisés. Ces outils ont pour but d'intégrer dans une seule application la gestion de l'identification/authentification et de l'habilitation/contrôle d'accès de multiples plate-formes et applications.
- Les solutions supportant l'ouverture de session simplifiée (accès unifié) sont de plus en plus répandues. L'ouverture de session simplifiée offre l'accès autorisé à des ressources multiples sans que la pré-autorisation de l'utilisateur soit nécessaire. Les infrastructures de gestion des privilèges dont il est question au paragraphe précédent, de même que Windows 2000 sont des exemples de solutions supportant cette fonctionnalité.
- L'utilisation de certificats d'attributs pour la spécification des rôles qu'un individu occupe ou des groupes auxquels il appartient est un mécanisme de contrôle d'accès aux applications et aux ressources faisant une avancée dans l'industrie. Le manque d'applications supportant pour l'instant l'émission et l'utilisation des certificats d'attributs est cependant un frein important à leur utilisation.

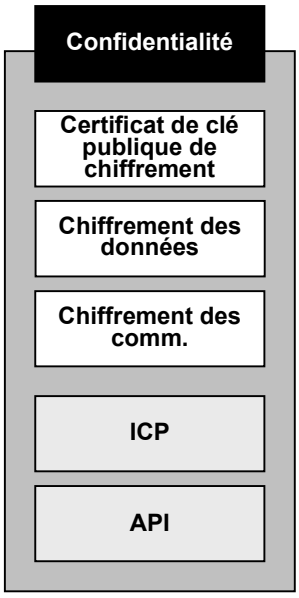
Règles architecturales

- **Donner accès aux utilisateurs aux ressources appropriées à leurs rôles et à leurs fonctions (G)**. Cette pratique permet de minimiser les impacts de la violation de la sécurité et permet un meilleur contrôle.
- **Dans la mesure du possible, réunir à l'intérieur d'une même solution la gestion des habilitations de toutes les applications d'une organisation (M et É)**. La gestion des habilitations est ainsi simplifiée.
- **Ne présenter aux utilisateurs que les ressources auxquelles ils ont l'autorisation d'accéder (G)**. Ceci évite de susciter la curiosité des utilisateurs.
- **Offrir une piste de vérification basée sur l'autorisation relative à l'utilisateur et aux ressources (G)**. Cette piste de vérification peut se faire via la journalisation ou la conservation des informations numérique.
- **Permettre le regroupement des ressources en catégories logiques en vue de reconnaître ou de refuser des droits d'autorisation (G)**, par exemple accorder l'accès à un groupe d'imprimantes dans un édifice.

Normes et standards

- ISO/IEC 10181-3
- **X.509 de l'UIT**
- SPKI de l'IETF
- **X.500 de l'UIT**
- DAP
- **LDAP**
- **IPSec de l'IETF**

2.5.5 Fonction de confidentialité



Description

La fonction de confidentialité assure qu'une information n'est pas divulguée ou mise à la disposition d'une entité (personne ou autre) ou d'un traitement non autorisé et ce, tout au long du cycle de vie de l'information si nécessaire.

Cette fonction inclut les mécanismes de sécurité et solutions technologiques suivants : certificat de clé publique de chiffrement, mécanismes de chiffrement des données et des communications, infrastructure à clés publiques (ICP) et interface de programmation d'applications (API).

Tendances de l'industrie

- Le chiffrement de données au niveau des applications de type SSL/TSL est sans nul doute le moyen de chiffrement le plus répandu puisqu'il est utilisé de façon massive sur Internet pour la transmission de données sensibles entre un fureteur et un serveur Web. Le chiffrement SSL à l'aide d'une clé de 128 bits tend à devenir la norme, particulièrement lorsque des données sensibles telles que des données monétaires sont échangées.
- Au niveau du chiffrement des messages électroniques, les produits supportant la norme S/MIME tels que Microsoft Outlook, Lotus Notes et Netscape Navigator sont en voie de remplacer la technologie Pretty Good Privacy qui s'est fait une modeste niche auprès de groupes de travail restreints dans certaines organisations. Cependant, certaines problématiques telles la gestion des clés de chiffrement ou le manque de compréhension des mécanismes par les utilisateurs potentiels freinent l'adoption de S/MIME et de toute technologie de chiffrement des messages électroniques d'ailleurs.
- La technologie de réseau privé virtuel (RPV) permettant la création d'un canal sécurisé (chiffré), généralement à l'intérieur d'Internet, gagne rapidement en popularité comme élément de base des infrastructures d'accès à distance des organisations, y remplaçant avantageusement les accès à distance (RAS) et les accès dédiés WAN. Les RPV, combinés à l'authentification forte, font actuellement une percée dans le secteur financier.

Règles architecturales

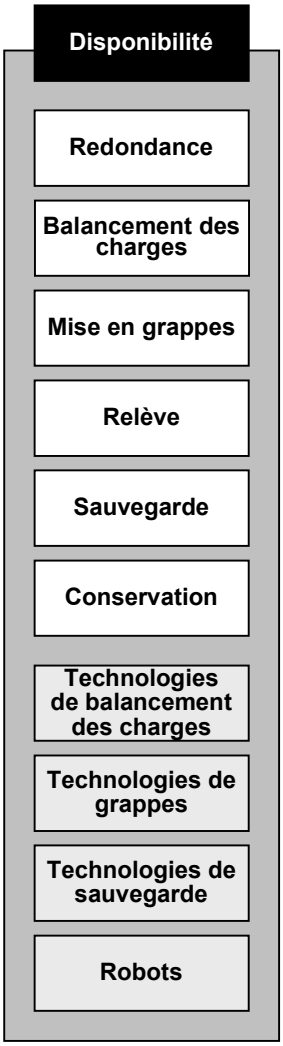
- **Offrir des applications ou commandes permettant aux utilisateurs de chiffrer/déchiffrer facilement des données (M et É)**.

- **Sécuriser les données sensibles circulant entre un client et un serveur à l'aide du protocole SSL ou de la technologie RPV (M et É)**.

Normes et standards

- ISO/IEC 10181-5
- L2TP
- **IPSec de l'IETF**
- **SSL/TLS de l'IETF**
- S/MIME de l'IETF
- XML Encryption du W3C
- **WTLS du ASP Forum**

2.5.6 Fonction de disponibilité



Description

La fonction de disponibilité assure que les informations numériques et les systèmes sont accessibles en temps voulu et de la manière requise par une entité autorisée (personne ou autre), et ce, si nécessaire, tout au long du cycle de vie de l'information.

Cette fonction inclut les mécanismes de sécurité suivants : la redondance des informations, applications et infrastructures, le balancement des charges, les technologies de grappes (clustering), la relève, la sauvegarde et la conservation des données.

Tendances de l'industrie

- L'expérience d'exploitation de nombreux sites de commerce entreprise à consommateur et entreprise à entreprise a permis de développer des méthodes et technologies évoluées garantissant la haute

disponibilité des applications Web transactionnelles. Ces technologies touchent autant la couche matérielle, que les couches système (système d'exploitation), réseau, serveur Web ou application. À titre d'exemple notons :

Couche matérielle

- Redondance géographique des infrastructures matérielles (capacité de relève en cas de désastre)
- Technologie RAID (Redundant Array of Independent Disks) pour la réplication des informations sur plusieurs disques durs

Couche réseau

- Redondance des liens et des fournisseurs de service de communication (en cas de panne d'un lien ou d'un fournisseur)
- Systèmes de gestion du trafic et de la bande passante permettant la gestion de la charge au niveau du réseau (par exemple PacketShaper de Packeteer, SynApps de Radware, Content-Intelligent Web Switches et Integrated Service Directors (iSD) de Alteon, Central Dispatch et Global Dispatch de Resonate)
- Optimisateurs de performance et de disponibilité (par exemple Big-IP Controller de F5)

Couche système

- Technologies de grappes permettant le passage des serveurs Web, d'applications et de bases de données d'un système à un autre en cas d'interruption.

Couche de serveur Web

- Redondance des serveurs Web
- Grappes de serveurs Web
- Technologies de balancement des charges intelligent
- Technique du balancement de charge de type « Round-Robin » que l'on retrouve dans les systèmes de noms de domaine (DNS)

Couche application

- Redondance des serveurs d'application
- Grappes de serveurs d'application et de serveurs de bases de données
- Réplication des transactions
- Réplication des bases de données
- Technologies de balancement des charges intelligent
- Distribution contrôlée du contenu permettant de rapprocher des utilisateurs le contenu de taille importante et qui nécessite un temps réponse faible. Akamai, Sandpiper et Adero offrent des solutions de ce type
- Réplication, sauvegarde et conservation des données

- La technique de balancement des charges de type « Round-Robin » que l'on retrouve dans les systèmes de noms de domaine (DNS) et qui est la plus commune n'est plus la seule technique de balancement des charges utilisée, ni celle qui est favorisée par les experts. En effet, cette technique qui permet la sélection aléatoire d'une adresse de serveur dans une liste d'adresses correspondant au même nom de site (exemple : www.alpha.com) est simple mais possède plusieurs faiblesses : 1) les DNS ne distinguent pas entre les serveurs disponibles ou non; 2) la mise à jour des listes (tables) DNS n'est pas dynamique; 3) les DNS ne tiennent pas compte de la taille des serveurs, de leur file d'attente

ou de l'utilisation de leur processeur. Les technologies de balancement des charges intelligent permettent de pallier à ces problématiques.

- L'atteinte d'un haut niveau de disponibilité étant très difficile, plusieurs méthodes de masquage des temps d'arrêts prévus ont été développées au cours des années afin de créer la perception d'une disponibilité ininterrompue : temps d'arrêts réguliers annoncés (par exemple, 4 heures par semaine de temps d'arrêt), disponibilité 24x7, mais pas sur certaines fonctions d'un site ou d'une application, masquage des effets des temps d'arrêts planifiés par la programmation (par exemple, les transactions peuvent être mises en file d'attente pour être traitées plus tard ou elles peuvent être redirigées temporairement vers une réplique du système principal).

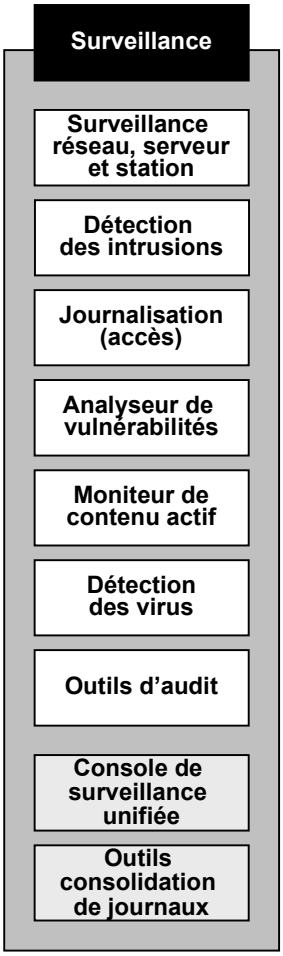
Règles architecturales

- **Fournir des mécanismes de redondance des infrastructures matérielles, applications et informations numériques (M et É).** Ceci, particulièrement dans le cas d'applications demandant un haut niveau de disponibilité.
- **Déployer des technologies de balancement des charges intelligent, minimalement au niveau des serveurs d'application Web (M et É).** Les serveurs d'application Web offrent pour la plupart ce type de technologie.

Normes et standards

Aucun

2.5.7 Fonction de surveillance



Description

La fonction de surveillance met en évidence les vulnérabilités, offre des pistes de vérification et permet la protection contre les tentatives d'intrusions et les programmes malicieux et ce, tout au long du cycle de vie de l'information si nécessaire.

Plus spécifiquement, cette fonction contient les mécanismes de sécurité et solutions technologiques suivants : les systèmes de surveillance des réseaux, serveurs et stations, les systèmes de détection des intrusions et des virus, la journalisation des accès, les analyseurs de vulnérabilité, les moniteurs de contenu actif, les outils d'audit, les consoles de surveillance unifiées et les outils de consolidation de journaux.

Tendances de l'industrie

- Les détecteurs d'intrusions, les systèmes d'analyse des vulnérabilités et les moniteurs de contenus actifs constituent en eux-mêmes de nouvelles tendances visant à complémenter les mécanismes de protection des réseaux fournis par les coupe-feu et les moyens de protection des informations fournis par les détecteurs de virus.
  - Les experts en sécurité recommandent l'utilisation conjuguée de systèmes de détection des intrusions sur les réseaux et de systèmes de détection des intrusions sur les serveurs. En effet, l'utilisation de ces approches fournit deux lignes d'avertissements et permet la détection d'attaques différentes.
  - Les systèmes d'analyse des vulnérabilités constituent un type d'outil particulièrement récent permettant de tester la robustesse des infrastructures technologiques et applications de sécurité. À la manière des détecteurs d'intrusions, les analyseurs de vulnérabilités sont basés sur deux approches : l'analyse des vulnérabilités basée sur les réseaux et sur les serveurs. Le premier type permet de simuler le comportement d'attaquants afin de mettre en évidence les faiblesses des systèmes qui sont testés. Les analyseurs de vulnérabilités basés sur les serveurs vérifient les paramétrisations des systèmes de façon à déterminer si elles sont consistantes avec les politiques de sécurité de l'organisation. Les experts recommandent l'utilisation conjuguée de ces deux types de produits.

  - Les détecteurs de virus sont de plus en plus complémentés par des moniteurs de contenus actifs permettant de détecter sur les ordinateurs ou les réseaux du contenu pouvant potentiellement faire des dommages (virus, Java et Active-X malicieux, etc.).

- Les systèmes de surveillance des réseaux, équipements de communication et serveurs permettent la paramétrisation, le monitorage et la correction des problèmes qui affaiblissent ces différentes infrastructures technologiques. Plusieurs systèmes de ce type, particulièrement les systèmes de surveillance des équipements de communication, sont très spécialisés et supportent uniquement les équipements d'un seul manufacturier et parfois même un seul type ou modèle d'équipement. Une nouvelle génération de produits vise cependant à intégrer dans un même produit ou dans une même console de gestion la surveillance de plusieurs types d'équipements. Cette tendance est représentée par des outils tels que la série CiscoWorks 2000. Ce dernier permet non seulement la gestion des équipements de communication de Cisco, mais aussi la gestion des équipements produits par d'autres fabricants à travers une interface commune.
- Plus récemment encore, d'autres type de consoles de surveillance ont vu le jour. Ces consoles de surveillance unifiées, appelées aussi « outils de prise de conscience de la sécurité en temps réel » (« Real-Time Security Awareness »), permettent aux gestionnaires de sécurité de gérer les diverses solutions de sécurité en temps presque réel à travers une console de gestion unifiée.
- Les détecteurs de virus sont certainement la technologie de surveillance la plus utilisée dans les organisations. Selon la firme Giga Information Group, les fournisseurs d'antivirus vont continuer d'améliorer l'approche traditionnelle de filtrage pour stopper les virus en développant de meilleurs systèmes pour l'identification des virus et la distribution des définitions de virus (par exemple Digital Immune System de Symantec). Les outils de gestion centralisés vont s'améliorer et l'approche de filtrage sera complémentée par des technologies alternatives telles que le blocage des comportements.

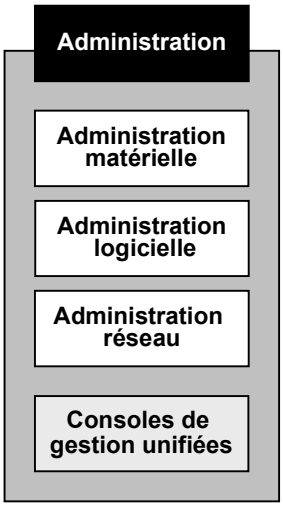
Règles architecturales

- **Utiliser des méthodes de surveillance permettant de couvrir à la fois les réseaux, les serveurs, les applications et les informations (M et É)**. En effet, ces divers éléments ne possèdent pas tous les mêmes vulnérabilités et les intrusions ne surviennent pas toutes par les réseaux ou les serveurs.
- **Réaliser une surveillance humaine des systèmes de surveillance (G)**. Comme la plupart des outils de surveillance ne sont justement que des outils de surveillance et non des outils d'intervention, un humain doit être prêt à intervenir pour gérer et corriger la situation.
- **Offrir une piste de vérification des ouvertures de sessions réussies et non-réussies (G)**.
- **Offrir une piste de vérification des accès aux informations numériques sensibles réussis et non-réussis (G)**.
- **Offrir une piste de vérification des transactions électroniques (M et É)**.

Normes et standards

- ISO/IEC 10181-7
- **SNMP**
- RMON
- RMON2

2.5.8 Fonction d'administration



Description

La fonction d'administration permet l'administration sécuritaire des logiciels, équipements informatiques et de réseautique tout au long du cycle de vie de l'information, si nécessaire. Elle inclut autant les processus (réalisation du schéma de configuration, inventaire, tenue des dossiers, etc.) que les outils.

Cette fonction contient les mécanismes de sécurité et solutions technologiques suivants : Administration des équipements, des logiciels et des réseaux (outils et processus) et console de gestion unifiée.

Tendances de l'industrie

- Une tendance importante semble se dessiner dans le monde de l'administration des ressources, soit l'intégration des outils de contrôle d'accès, des outils d'administration, de même que des outils de surveillance des applications, équipements informatiques et de réseautique, dans une seule et même console de gestion unifiée. Cette tendance est représentée par des outils tels que SMS de Microsoft, Unicenter TNG de Computer Associates et Tivoli d'IBM.

Règles architecturales

- Dans la mesure du possible, **l'administration des équipements, logiciels et réseaux devrait se faire de manière centralisée à l'intérieur des organisations (G)**.

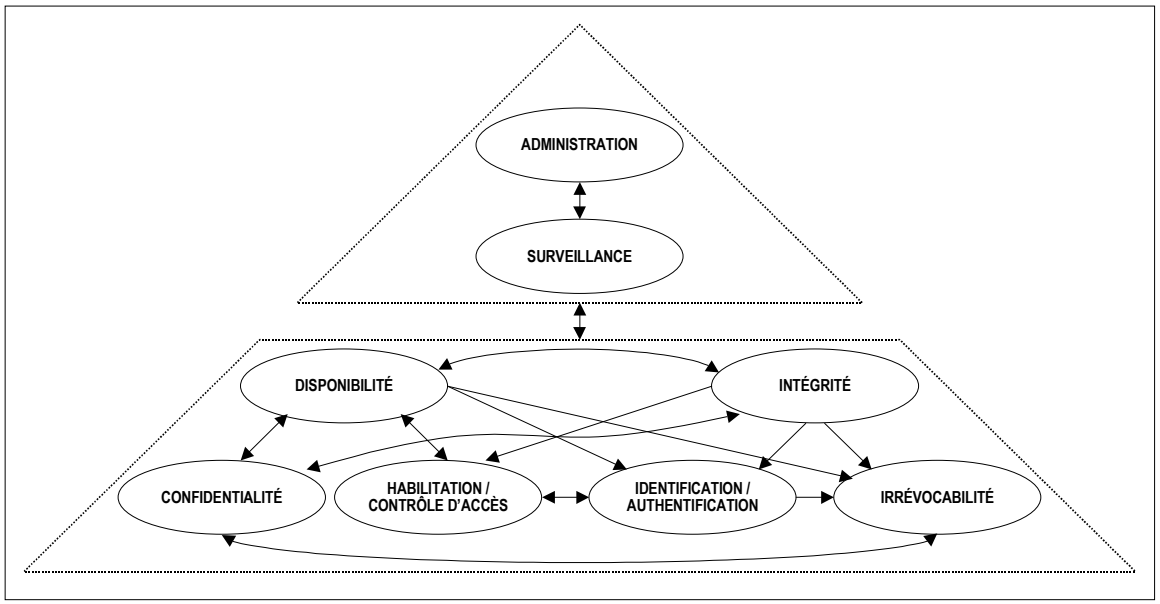
Normes et standards

- WBEM/CIM du DMTF
- **SNMP**
- RMON
- RMON2

2.5.9 Dépendances entre les fonctions de sécurité

Tel que la figure suivante le démontre, il existe de nombreuses dépendances entre les diverses fonctions de sécurité décrites précédemment. Ces dépendances tendent à démontrer que l'on ne peut envisager d'utiliser seules les différentes fonctions et mécanismes de sécurité. La figure « Dépendances entre les fonctions de sécurité » prend aussi bien en considération la sécurité des informations numériques que des applications, des équipements et des réseaux.

DÉPENDANCES ENTRE LES FONCTIONS DE SÉCURITÉ



La partie supérieure de la figure illustre la dépendance entre les fonctions d'administration et de surveillance. De plus, elle démontre clairement que les fonctions d'administration et de surveillance chapeautent l'ensemble des autres fonctions de sécurité.

Les fonctions d'administration et de surveillance sont intimement liées. Il est difficilement envisageable d'administrer des applications ou infrastructures technologiques qui ne sont pas surveillées. Il est tout aussi difficile de surveiller des applications ou infrastructures technologiques qui ne sont pas administrées de façon sécuritaire. Certains mécanismes et solutions technologiques remplissent d'ailleurs les deux fonctions.

Ainsi, ces deux fonctions de sécurité couvrent plus particulièrement les aspects de la gestion de la sécurité. La norme ISO/IEC 13335, qui se veut un guide pour la gestion de la sécurité des technologies de l'information, ainsi que le Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise[69] couvrent certains des éléments à considérer pour ces fonctions.

La partie inférieure présente les fonctions de sécurité applicables à la protection de l'information numérique, des applications, des équipements et des réseaux. Ce découpage des fonctions de sécurité s'inspire largement de la norme ISO/IEC 10181 qui établit un cadre permettant de spécifier les fonctions de sécurité pour les systèmes ouverts.

Il est à noter que chacune des fonctions de sécurité est en soi complète et que malgré les dépendances illustrées, des choix technologiques peuvent amener un regroupement causé par des exigences de gestion.

[69] On consultera le document *Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise* (février 2001) basée sur la norme ISO/IEC 13335 produit par le SCT pour plus d'informations.

À titre d'exemple, au niveau de la fonction d'irrévocabilité, nous pouvons observer que :

- L'irrévocabilité est dépendante de l'identification/authentification :
  - Si l'utilisateur d'un système n'est pas identifié/authentifié au niveau approprié, on ne peut garantir l'irrévocabilité d'une action ou d'une transaction.
- L'irrévocabilité est dépendante de la confidentialité :
  - Si la confidentialité de l'information peut être mise en doute (ex. qu'elle a été manipulée ou volée), on ne peut garantir l'irrévocabilité d'une action ou d'une transaction.

Enfin, il apparaît important de mentionner qu'en fonction du contexte d'utilisation des fonctions de sécurité (i.e. sécurité de l'information numérique, des applications, des équipements et/ou des réseaux) certaines dépendances seront plus ou moins fortes et parfois inexistantes.

2.6 L'information numérique au gouvernement du Québec

Cette section présente brièvement la démarche pour catégoriser l'information numérique, de même que les mécanismes de sécurité et solutions technologiques supportant la valeur de l'information numérique. De plus, elle décrit les relations existantes entre les mécanismes de sécurité et les solutions technologiques et le cycle de vie de l'information.

2.6.1 La valeur des attributs l'information numérique

À l'intérieur du « Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité », le SCT explique le contexte et la démarche pour catégoriser l'information numérique et établir les mesures de sécurité à mettre en place selon le contexte d'utilisation. Les travaux du SCT ont permis de dégager une démarche qui se résume en trois grandes étapes :

Étape 1 : Décider de l'information à catégoriser

Étape 2 : Catégoriser ces informations

Étape 3 : Déterminer les mesures à appliquer pour protéger les informations en fonction de la catégorisation désirée

Les informations à catégoriser retenues font l'objet d'une évaluation sur les attributs DICAI qui font partie des principes directeurs de la directive et qui sont : la disponibilité (**D**), l'intégrité (**I**n), la confidentialité (**C**), l'authentification (**A**) et finalement l'irrévocabilité (**I**r). On précise également le contexte d'utilisation des informations. En effet, pour une même information, les mesures de sécurité peuvent effectivement varier selon le contexte. Tel que le démontre le tableau « Valeurs des attributs », le SCT a défini 3 niveaux de sécurité élaborés en fonction des critères de DICAI.

VALEURS DES ATTRIBUTS

	Élevée	Moyenne	Basse
Disponibilité - Intolérance au délai	En tout temps	En terme de jours	En terme de semaines
Intégrité - Intolérance à la modification sans autorisation	Information exacte et intégrale en tout temps	Information exacte en tout temps	S/O
Confidentialité – Intolérance à la divulgation	Imposée par la loi	La loi laisse le choix à l'organisme	Publique
Authentification – Identification des parties	Formelle de toutes les parties	Formelle de l'une des parties	S/O
Irrévocabilité – Confirmation de l'exécution complète d'un échange	Probante essentielle	Démontrée utile	S/O

2.6.2 Mécanismes et solutions technologiques supportant la valeur de l'information numérique

Les différents mécanismes de sécurité et solutions technologiques présentés à la section 2.5 doivent être choisis entre autres en fonction de la valeur des différents attributs du DICAI. Ainsi, certains de ces mécanismes et solutions offrent, par exemple, un niveau d'identification/authentification ou d'intégrité élevée alors que d'autres offrent un niveau moyen ou faible. Le choix d'un mécanisme de sécurité ou d'une solution technologique peut aussi varier en fonction du contexte d'utilisation.

Le tableau « Mécanismes et solutions technologiques à utiliser selon la valeur des attributs » présente les mécanismes de sécurité et solutions technologiques potentielles pour assurer la sécurité des informations selon les différents attributs. Notons qu'en accord avec les diverses fonctions de sécurité présentées à la section 2.5, trois attributs (fonctions) ont été ajoutés aux cinq attributs du DICAI, soit l'habilitation/contrôle d'accès, la surveillance et l'administration. L'échelle de valeur incluse dans ce tableau s'inspire de celle utilisée dans le « Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité[70] » et présentée précédemment.

Afin de faciliter la lecture du tableau, les éléments suivants sont à considérer :

- Les solutions technologiques sont entre parenthèses alors que les mécanismes de sécurité ne le sont pas ;
- Les mécanismes de sécurité et solutions technologiques devant minimalement être mis en place pour assurer chacune des valeurs des attributs sont indiqués en gras. Ceux qui ne sont pas en gras sont optionnels et dépendent largement du contexte ;

[70] Le tableau du guide de catégoriation diffère légèrement du tableau « Mécanismes et solutions technologiques à utiliser selon la valeur des attributs » présenté à la page suivante. Le guide de catégorisation de l'information numérique devrait être revu en fonction du tableau de l'AGSIN.

- Les « ou » désignent des mécanismes et solutions technologiques alternatifs. Par exemple, afin de réaliser un niveau élevé d'identification/authentification, on utilisera, en plus d'un mot de passe, un jeton ou une carte à puce ou un certificat de clé publique de signature ou de la biométrie et des outils d'ouverture de session;
- Les « et » désignent des mécanismes et solutions technologiques complémentaires. Par exemple, afin d'assurer un niveau élevé d'intégrité, on utilisera les mécanismes de base des applications et des communications et (peut-être) une empreinte numérique ou un code d'authentification de messages et un certificat à clé publique de signature.
- Les crochets entourant les mécanismes et solutions technologiques regroupent en un ensemble des items alternatifs. Chaque item d'un ensemble est complémentaire aux items qui suivent ou qui précèdent dans la liste. Par exemple, au niveau de l'intégrité élevée, l'empreinte numérique (ou le code d'authentification de messages) est complémentaire aux mécanismes de base des applications et des communications.

Il est à noter que l'ICP est la solution privilégiée par le SCT lorsque le contexte d'utilisation est favorable à cette solution.

MÉCANISMES ET SOLUTIONS TECHNOLOGIQUES À UTILISER SELON LA VALEUR DES ATTRIBUTS

	Élevée	Moyenne	Basse
Intégrité	**Mécanismes de base des applications et des communications** et { CAM ou Empreinte numérique } et Certificat de clé publique de signature (ICP, répertoire)	**Mécanismes de base des applications et des communications** et { CAM ou Empreinte numérique }	**Mécanismes de base des applications et des communications**
Irrévocabilité	**Journalisation (outils de consolidation des journaux)** et **Conservation** et **Certificat de clé publique de signature (ICP)** et Notarisation	**Journalisation** et **Conservation**	**Journalisation**

	Élevée	Moyenne	Basse
Identification/ Authentification	**Jeton** ou **Carte à puce – avec certificat de clé publique de signature (ICP, répertoire)** ou **Certificat de clé publique de signature (ICP, répertoire)** et **Mot de passe** ou **Biométrie** et (Outils d'ouverture de session simplifiée)	**Jeton** ou **Carte à puce** ou **Certificat de clé publique de signature (ICP, répertoire)** et **Mot de passe** et (Outils d'ouverture de session simplifiée)	**Code d'usager/Mot de passe** ou **NIP**
Habilitation/ Contrôle d'accès	**Mécanismes des systèmes d'exploitation et applications** ou **Certificat d'attribut (ICP, répertoire)** et **Coupe-feu** et (Infrastructures de gestion des privilèges)	**Mécanismes des systèmes d'exploitation et applications** et **Coupe-feu**	**Mécanismes des systèmes d'exploitation et applications**
Confidentialité	**Chiffrement par RPV** ou **Chiffrement des communications 128 bits** ou **Chiffrement des données 128 bits** et **Certificat de clé publique de chiffrement (ICP, répertoire)**	**Chiffrement des données 128 bits** ou **Chiffrement des communications 128 bits**	Chiffrement des données 40 bits ou Chiffrement des communications 40 bits
Disponibilité	**Relève active** et **Sauvegarde** et **Conservation** et **Redondance** et Balancement des charges et Technologies de grappes	**Relève passive** et **Sauvegarde** et **Conservation** et Redondance	**Relève passive** et **Sauvegarde** et Conservation

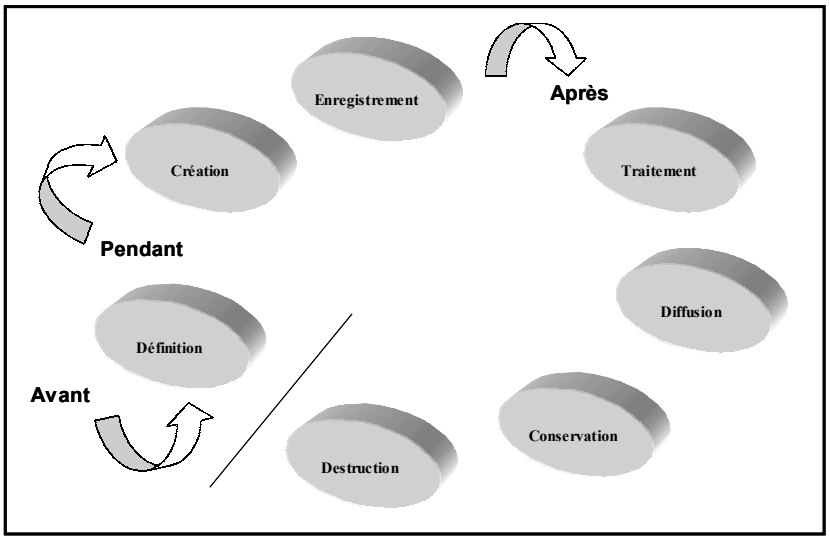
	Élevée	Moyenne	Basse
Surveillance	**Détection des virus** et **Journalisation (outils de consolidation des journaux)** et **Détection des intrusions** et **Outils d'audit** et **Outils de surveillance réseaux, serveurs et stations** et **Analyseur de vulnérabilités** et **Moniteur de contenu actif**	**Détection des virus** et **Journalisation** et **Détection des intrusions** et Outils d'audit et Outils de surveillance réseaux, serveurs et stations et Analyseur de vulnérabilités et Moniteur de contenu actif	**Détection des virus** et **Journalisation** et Outils d'audit
Administration	**Outils d'administration matérielle, logicielle et réseau intégrés**	**Outils d'administration matérielle, logicielle et réseau intégrés**	**Outils d'administration matérielle, logicielle et réseau de base**

Note : le chiffrement des communications réfère aux mécanismes et/ou solutions technologiques lors des communications. Le chiffrement des données quant à lui réfère aux mécanismes et/ou solutions technologiques sur les médias de stockage.

2.6.3 Mécanismes et solutions technologiques durant le cycle de vie de l'information

Les mécanismes de sécurité et solutions technologiques mis en place pour assurer la sécurité de l'information peuvent varier en fonction des étapes du cycle de vie de cette information décrites dans la figure suivante :

CYCLE DE VIE DE L'INFORMATION



En fait, cette variation est occasionnée par une modification du niveau de sécurité de l'information numérique le long du cycle de vie. Pour illustrer cette variation, utilisons deux scénarios fictifs :

Exemple1 : Information nécessitant un niveau de sécurité élevé tout au long de son cycle (ex. renseignements personnels)

	Définition	Création	Enregistre-ment	Traitement	Diffusion	Conserva-tion	Destruc-tion
Intégrité	M	É	É	É	É	É	N/A
Irrévocabilité	M	É	É	É	É	N/A	É
Identification/ Authentification	M	É	N/A	É	É	N/A	É
Habilitation/ Contrôle d'accès	M	É	N/A	É	É	N/A	É
Confidentialité	M	É	É	É	É	É	É
Disponibilité*	M	É	É	É	É	M	B
Surveillance	M	É	É	É	É	É	É
Administration	M	É	É	É	É	É	É

É : élevée M : moyenne B : basse N : nulle N/A : non applicable

* Le niveau de disponibilité n'est pas uniquement lié à la valeur de l'information mais aussi à des exigences d'affaires.

Exemple 2 : Information nécessitant un niveau de sécurité moyen en début de cycle de vie mais de plus faible vers la fin (ex. budget).

	Définition	Création	Enregistre-ment	Traitement	Diffusion	Conserva-tion	Destruc-tion
Intégrité	M	M	M	M	M	B	B
Irrévocabilité	B	B	B	B	N	N/A	N
Identification/ Authentification	M	M	N/A	M	M	N/A	B
Habilitation/ Contrôle d'accès	M	M	M	M	M	N/A	B
Confidentialité	M	M	M	M	M	B	N
Disponibilité*	M	É	É	M	M	B	B
Surveillance	M	M	M	M	M	B	B
Administration	M	M	M	M	M	B	B

É : élevée M : moyenne B : basse N : nulle N/A : non applicable

* Le niveau de disponibilité n'est pas uniquement lié à la valeur de l'information mais aussi à des exigences d'affaires.

Dans une situation où le niveau de sécurité de l'information varie en fonction des différentes étapes du cycle de vie de l'information, l'architecte responsable de la sécurité aura recours à l'une ou l'autre des stratégies principales suivantes :

- Pour chaque fonction de sécurité dont la valeur des attributs de l'information numérique varie, avoir recours à des mécanismes de sécurité et solutions technologiques différents pour chaque niveau de sécurité. Par exemple, si on prend comme base de travail l'exemple numéro 2:
  - **Identification/authentification** : La définition, la création, le traitement et la diffusion des informations numériques font appel à des mécanismes de niveau moyen (jeton et mot de passe, carte à puce et mot de passe, certificat et mot de passe, etc.) alors que la destruction des informations ne fait appel qu'à des mécanismes de bas niveau (mot de passe, NIP).
  - **Irrévocabilité** : La définition, la création, l'enregistrement et le traitement des informations numériques font appel à des mécanismes de bas niveau (journalisation, conservation) alors que la diffusion, la conservation et la destruction ne nécessitent aucun mécanisme de sécurité assurant l'irrévocabilité.
  - Etc.
- Pour chaque fonction de sécurité, avoir recours aux mécanismes de sécurité correspondant à la valeur des attributs de l'information numérique la plus élevée du cycle de vie. Par exemple, si on prend comme base de travail l'exemple numéro 2 :
  - **Identification/authentification** : Toutes les étapes du cycle de vie de l'information qui nécessitent de l'identification/authentification font appel à des mécanismes de niveau moyen (jeton et mot de passe, carte à puce et mot de passe, certificat et mot de passe, etc.).
  - **Confidentialité** : Toutes les étapes du cycle de vie qui nécessitent de la confidentialité font appel à des mécanismes de niveau moyen (chiffrement des données 128 bits).
  - Etc.

Notons que cette dernière approche n'est pas celle qui est préconisée dans la présente architecture. Cependant, le contexte d'utilisation pourra nécessiter dans certains cas particuliers l'utilisation d'une telle approche.

2.7 Le modèle général de l'AGSIN

La présente section définit les modalités relatives à l'AGSIN. Elle positionne le modèle général de l'AGSIN et introduit les concepts qui doivent être mis de l'avant par l'ensemble des intervenants de l'appareil gouvernemental québécois, de façon à ce que chaque entité concernée puisse adapter, mettre en œuvre (implanter) et appliquer les éléments de l'AGSIN dans leur architecture de sécurité de l'information numérique respective.

2.7.1 Positionnement de l'AGSIN dans l'AEG

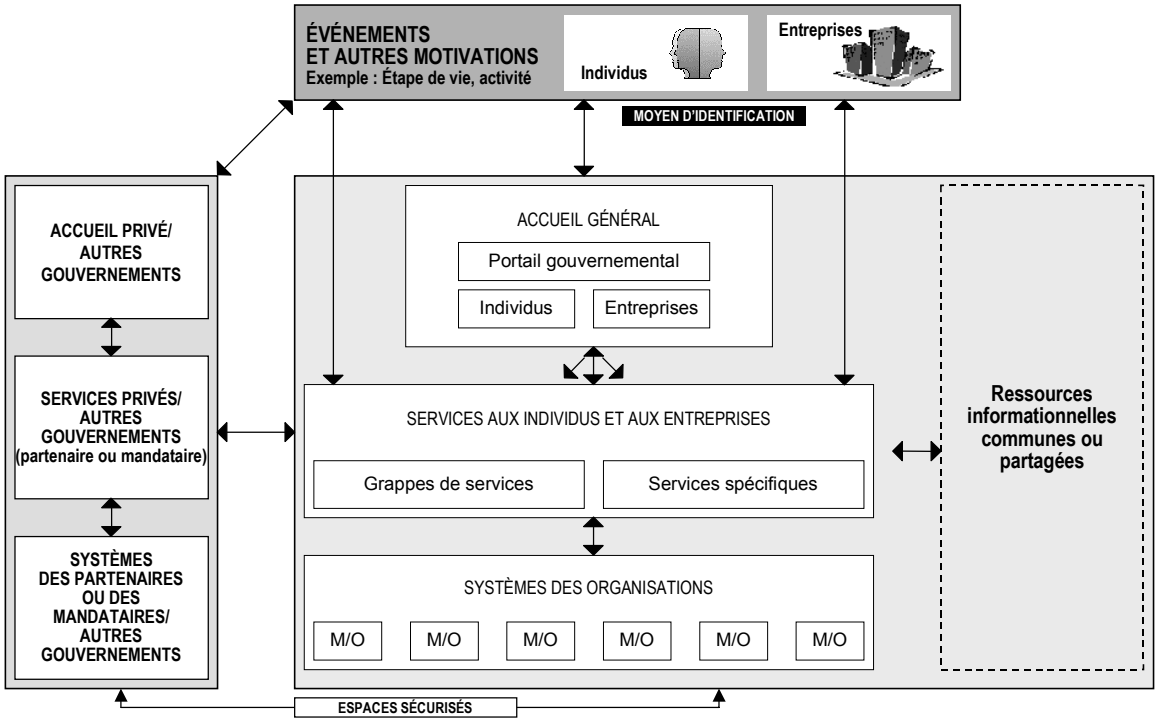
2.7.1.1 Le modèle général de PES

L'AGSIN étant un segment de l'AEG, le modèle général de prestation électronique de services élaboré dans la première version de l'AEG définissant globalement le processus de prestation électronique de services aux individus et aux entreprises est présenté. Il met en lumière les éléments entrant en jeu dans ce processus et illustre les interactions possibles entre ces éléments, de même que le concept d'espace sécurisé[71].

[71] On se référera au document *Architecture d'entreprise gouvernementale, Contexte, perspective et architecture de haut niveau* définissant les concepts de l'AEG pour plus d'informations.

MODÈLE GÉNÉRAL DE LA PES

(REPRIS DE L'AEG)

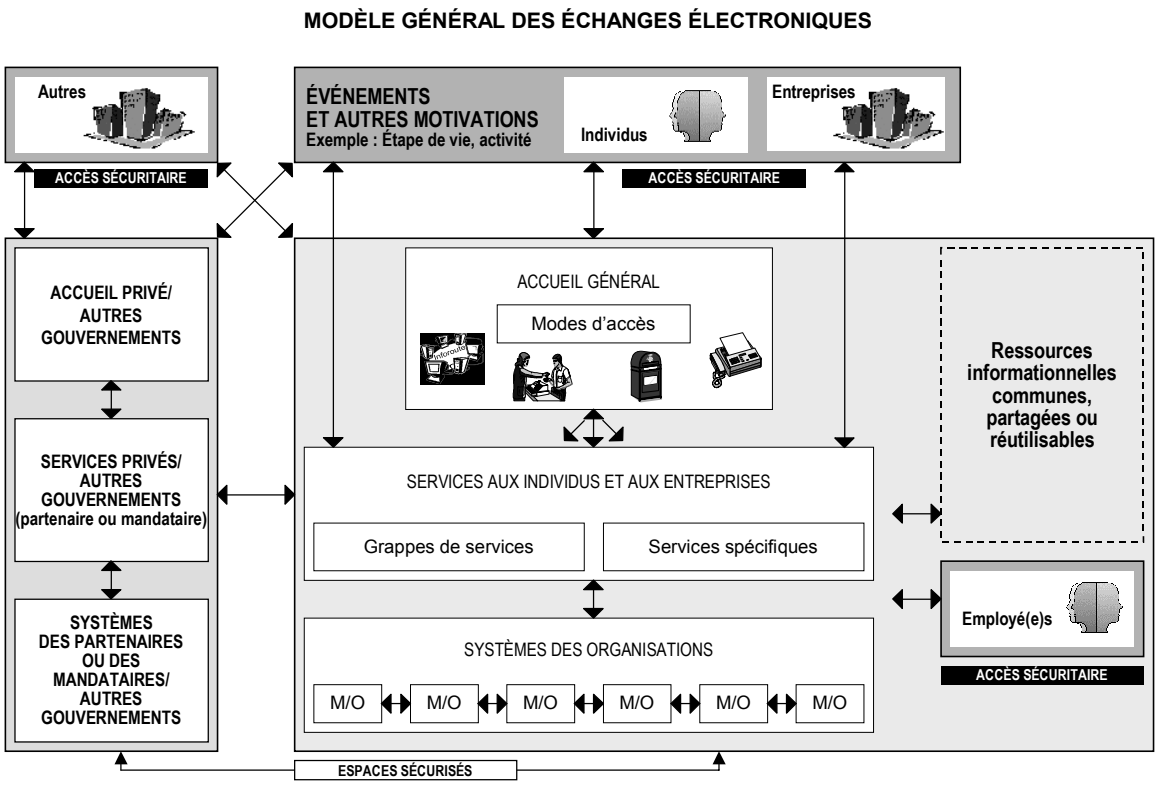


La figure précédente illustre le modèle général de la PES de la première version de l'AEG qui s'est concentrée sur la prestation électronique de services aux individus et entreprises.

2.7.1.2 Le modèle général des échanges électroniques (PES élargie)

L'AGSIN ayant une portée plus large que la première version de l'architecture d'entreprise gouvernementale, le modèle général de la PES de cette dernière a été adapté afin d'inclure :

- les services aux autres clientèles (partenaires, mandataires, fournisseurs, autres gouvernements, etc.);
- les services aux employé(e)s;
- les interactions entre les M/O;
- les accès sécuritaires (élargissement de moyen d'identification);
- les différents modes d'accès (élargissement de portail gouvernemental).



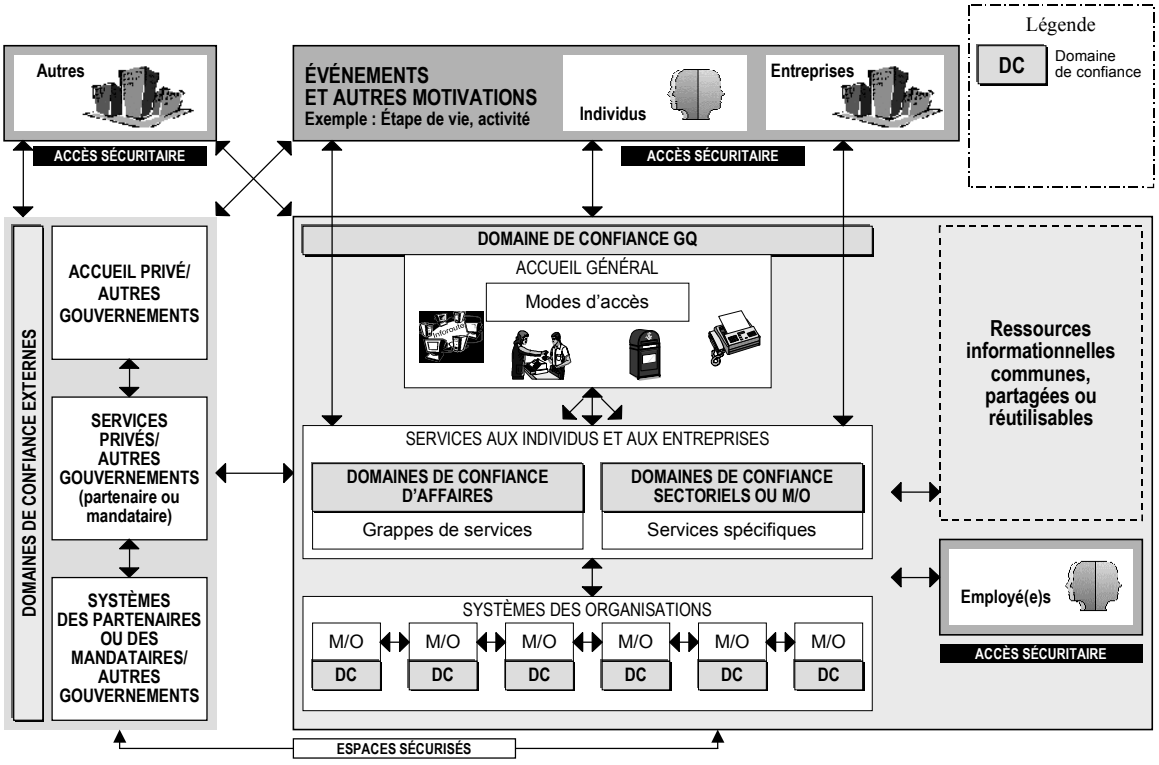
La figure précédente illustre le modèle général de la PES adapté à la portée de l'AGSIN soit le modèle général des échanges électroniques (ÉÉ). Elle présente une vue d'ensemble de la prestation électronique de services aux individus, entreprises, employé(e)s et autres clientèles.

2.7.1.3 Le modèle général des ÉÉ protégés

Les adaptations apportées au modèle général de la PES permettent de faire le lien entre la vision d'affaires de l'AEG et la vision de la sécurité de l'information numérique préconisée par l'AGSIN. Ce lien s'établit grâce au concept de domaines de confiance[72].

[72] Le concept de Domaine de confiance est défini à la section 2.7.2 et décrit à la section 2.7.2.1.

MODÈLE GÉNÉRAL DES ÉCHANGES ÉLECTRONIQUES PROTÉGÉS



La figure précédente illustre le modèle général des ÉÉ protégés et introduit le concept de domaines de confiance. Elle illustre, de manière uniforme à tous les intervenants, la réalité de l'appareil gouvernemental québécois en matière de sécurité.

Au niveau gouvernemental, chaque M/O ou organisation responsable d'un secteur, d'une grappe de services ou d'un service gouvernemental commun établit, dans le cadre de ses activités, des relations d'affaires qui nécessitent des mesures de sécurité afin de protéger adéquatement les informations dont il est responsable. Il en va de même avec le secteur privé qui interagit avec l'appareil gouvernemental mais n'est pas sous sa gouvernance.

À cette fin, le modèle général des ÉÉ protégés propose quatre types de domaines de confiance sous la gouverne du gouvernement du Québec :

- les domaines de confiance des M/O (ex.: MJQ, SAAQ, etc.);
- les domaines de confiance d'affaires (ex.: MIC pour la trousse de démarrage d'entreprise, etc.);
- les domaines de confiance sectoriels (ex.: Secteur de la santé, etc.)[73];
- le domaine de confiance du gouvernement du Québec (GQ) (ex.: Infrastructure commune au niveau des services gouvernementaux (SG), gouvernance au niveau du SCT, etc.);

[73] Des travaux additionnels dans le cadre de l'AEG sont nécessaires afin de définir de manière uniforme le concept de secteur gouvernemental.

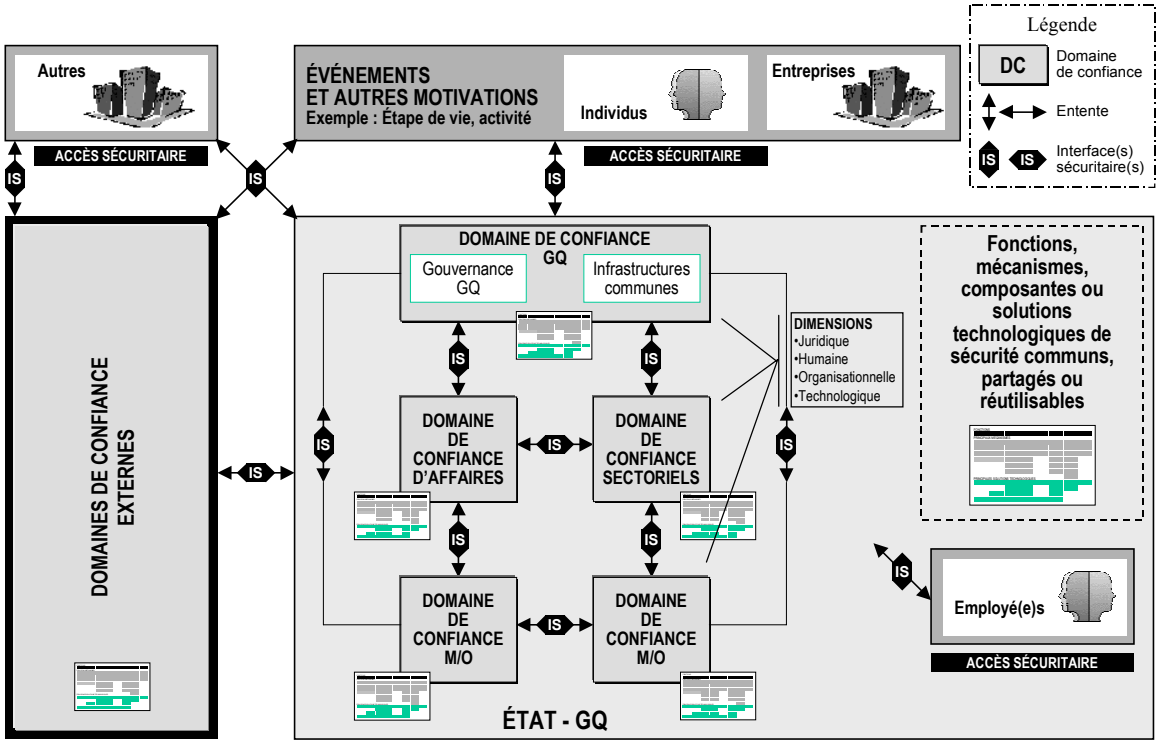
Le gouvernement du Québec interagissant non seulement entre les entités sous sa gouvernance mais également avec des entités externes, un cinquième type de domaine de confiance est proposé :

- les domaines de confiance externes (ex.: Secteur privé, secteur financier, gouvernement du Canada, etc.).

2.7.2 Le modèle général de l'AGSIN

En s'inspirant du formalisme et des concepts du modèle général des ÉÉ protégés, le modèle général de l'AGSIN présenté dans la figure suivante, fait ressortir les interactions entre les domaines de confiance et les clientèles visées. Les domaines de confiance sont définis et encadrés par les différents aspects des dimensions juridique, humaine, organisationnelle et technologique et couvrent toutes les étapes du cycle de vie de l'information.

MODÈLE GÉNÉRAL DE L'AGSIN
VUE – AFFAIRES



Ce modèle a l'avantage :

- d'assurer une vision commune en matière de sécurité au sein de l'appareil gouvernemental québécois;
- de permettre le positionnement des M/O et des organisations responsables d'un secteur, d'une grappe de services ou d'un service gouvernemental commun dans le modèle général de l'AGSIN afin de favoriser leur adhésion au modèle;
- de présenter de manière simple la complexité des relations entre les domaines de confiance et avec les clientèles;

- de maintenir l'autonomie des M/O et des organisations responsables d'un secteur, d'une grappe de services ou d'un service gouvernemental commun au niveau de la sécurité en fournissant des lignes directrices en cette matière;
- de délimiter les champs de compétence en matière de sécurité des M/O et des organisations responsables d'un secteur, d'une grappe de services ou d'un service gouvernemental commun;
- de permettre une meilleure interopérabilité en uniformisant les façons de faire et les interactions;
- d'offrir l'ouverture et la souplesse nécessaires afin de permettre l'évolution de l'AGSIN en fonction des nouveaux besoins gouvernementaux.

Le modèle général de l'AGSIN se base sur un ensemble d'éléments dont notamment :

- le document orientations et principes[74] en matière de sécurité de l'information numérique afin d'assurer l'authentification, la confidentialité, l'intégrité, la disponibilité et l'irrévocabilité de l'ensemble de l'information numérique dans le fonctionnement de l'État et dans la relation de l'État avec les individus, les partenaires, les mandataires, les fournisseurs ou toute autre entité et ce, durant tout le cycle de vie de l'information[75];
- le document portrait et besoins gouvernementaux[76] en matière de sécurité de l'information numérique afin d'assurer l'alignement de l'AGSIN avec les tendances de l'industrie et gouvernementale hors Québec et de couvrir adéquatement les besoins en matière de sécurité de l'appareil gouvernemental québécois;
- la norme ISO/IEC 10181[77] qui établit un cadre permettant de spécifier les fonctions de sécurité pour les systèmes ouverts;
- La norme ISO/IEC 13335 qui se veut un guide pour la gestion de la sécurité des technologies de l'information.;
- la norme ISO 7498-2[78]qui établit un cadre permettant de coordonner le développement des normes existantes et à venir pour l'interconnexion des systèmes;
- le Manuel canadien de la sécurité des technologies de l'information[79] qui explique les notions importantes, l'analyse coûts-avantages et les rapports mutuels des mesures de protection de la sécurité TI. On y trouve l'illustration des avantages qu'offrent ces mesures, les principales techniques ou approches propres à chacune d'entre elles et d'importantes considérations connexes.

[74] On consultera pour plus d'informations le document *Architecture gouvernementale de la sécurité de l'information numérique – Orientations et principes* reprenant les éléments de l'AEG et énonçant un nombre de principes en complémentarité à ceux existants.

[75] L'AGSIN ne couvre que l'information numérique mais il est acquis que le gouvernement veille à la sécurité de l'information dans son ensemble peu importe le support.

[76] On consultera pour plus d'informations le document *Architecture gouvernementale de la sécurité de l'information numérique - Portrait et besoins gouvernementaux* décrivant les tendances de l'industrie et les tendances gouvernementales hors Québec en ce qui a trait à la sécurisation de l'information. Ce même document présente également le contexte gouvernemental québécois, de même que l'état actuel de la situation en matière de sécurité dans les ministères et organismes consultés, les chantiers centraux et les infrastructures centrales. Il présente aussi leurs besoins de sécurité.

[77] On se référera à l'annexe D et à la norme ISO/IEC 10181 pour plus d'informations.

[78] On se référera à l'annexe D et à la norme ISO 7498-2 pour plus d'informations.

[79] On consultera le *Manuel canadien de la sécurité des technologies de l'information* pour plus de détails.

Le modèle général de l'AGSIN implique un nombre de concepts fondamentaux en matière de sécurité qui sont décrits en détails dans les sections suivantes. Cependant, afin de faciliter une compréhension commune de tous les intervenants impliqués, une définition de ces concepts est présentée ci-dessous.

Domaine de confiance (DC) :

Un domaine de confiance se définit comme un ensemble d'éléments d'ordre juridique, humain, organisationnel et technologique, un cadre de gestion de la sécurité et un ensemble d'activités pertinentes à la sécurité qui sont tous assujettis à une politique de sécurité administrée par une seule autorité en matière de sécurité[80].

Entente (E) :

Une entente définit les règles qui régissent les interactions entre les domaines de confiance ainsi qu'avec les clientèles[81]. Elle permet également de délimiter les champs de compétence entre les domaines de confiance. Une entente contient au minimum une Interface sécuritaire.

Interface sécuritaire (IS) :

Une interface sécuritaire définit les modalités techniques de sécurisation de l'information numérique. Elle est un ensemble d'éléments, comprenant à la fois des aspects logiciels et matériels, qui présente les normes et standards et les fonctions et mécanismes de sécurité nécessaires pour assurer la connectivité et l'interopérabilité entre les domaines de confiance ainsi qu'avec les clientèles[82].

Tel que présenté à la section 2.4, la sécurité de l'information numérique repose sur un certain nombre de moyens juridiques, humains, organisationnels et technologiques. Ce sont ces mêmes dimensions qui sont à la base d'un domaine de confiance. La politique de sécurité définit les responsabilités et les règles générales applicables au domaine de confiance. Chaque domaine de confiance possède sa propre politique de sécurité et élabore un cadre de gestion correspondant en s'assurant de couvrir l'ensemble des dimensions de la sécurité.

L'AGSIN présente les fonctions de sécurité, les mécanismes de sécurité et les solutions technologiques nécessaires pour assurer un niveau adéquat de sécurité de l'information numérique tout au long de son cycle de vie tel que présenté dans la section 2.5. Ce sont ces mêmes fonctions de sécurité qui, au besoin, sont à la base des accès sécuritaires entre le gouvernement du Québec et les différentes clientèles.

L'AGSIN ne présuppose pas l'utilisation de produits particuliers en matière de sécurité mais propose des mécanismes et des composantes ou solutions technologiques conformes aux normes et standards ayant fait leurs preuves sur le marché afin de supporter les fonctions de sécurité. À cet effet, des spécifications techniques doivent être définies pour sélectionner les produits qui supporteront les ÉÉ protégés.

Selon la firme Gartner[83], les organisations doivent planifier en fonction de l'hétérogénéité et être sélectives dans l'application des architectures technologiques. Les standards doivent être mis à jour régulièrement.

[80] La définition de domaine de confiance est inspirée de la norme ISO/IEC 10181-1
[81] La définition d'entente est inspiré de la norme ISO/IEC 10181-1
[82] La définition d'interface sécuritaire est inspirée du document *Orientations pour l'architecture IDA* de la Commission européenne.
[83] Hypothèse de planification stratégique. *La réalité des travaux d'architecture*, Gartner Group, 2001.

L'architecture technologique doit permettre une variété de standards alternatifs afin d'accommoder différents contextes. Ainsi :

- Les organisations vont rarement être capables d'appliquer des standards d'architecture technologique pour atteindre une pleine uniformité pan-entreprise; pour plus de 90 % des composantes technologiques, une grande entreprise utilisera plus d'un produit matériel ou logiciel jusqu'à environ 2005 (probabilité 0,9). Gartner base ces informations sur le fait que :
  - Les architectures de TI classiques ont été spécifiées dans un monde où les organisations centrales des TI ont conçu et possédé toutes les applications, et par conséquent, où elles contrôlaient les technologies;
  - Les architectures de TI modernes doivent être davantage vues comme des règles d'urbanisme que comme une « liste d'épicerie » stricte. L'objectif des règles d'urbanisme est de vérifier la qualité et non pas d'atteindre l'uniformité. Une architecture technologique peut réduire, mais pas éliminer, l'hétérogénéité. Aucun standard technologique ne peut être appliqué à toutes les applications, à tous les départements/organisations ou à tout moment. Les applications diffèrent souvent suffisamment pour justifier différents matériels et logiciels;
  - La notion d'uniformité est irréaliste dans un monde où l'informatique est incorporée à tellement d'outils différents. Lorsqu'un progiciel entre en conflit avec les standards corporatifs d'architecture, le standard sera généralement rejeté.

Toujours selon Gartner, la vitesse de changement observée dans les organisations rend souvent les documents d'architecture technologique obsolètes avant même que leur encre n'ait séchée! Une approche organisationnelle plus dynamique permet d'intégrer les architectures d'affaires et de systèmes d'information sur une base continue. En d'autres mots, le succès d'une architecture, quelle qu'elle soit, repose davantage sur les mécanismes mis en place pour l'actualiser que sur son contenu spécifique.

À cet effet, l'AGSIN doit faire partie d'un processus continu et évolutif sous la gouvernance de l'État et ne doit pas être considérée comme un « autre » document d'architecture. Elle se veut un guide facilitant l'élaboration des architectures de sécurité de l'information numérique détaillées en attirant l'attention sur la nécessité de :

- La reconnaissance d'intervenants multiples, à des niveaux de confiance différents, dans des rôles différents, etc. Les sections suivantes explicitent les concepts de l'AGSIN relié à cette nécessité;
- La sélection et l'implantation des fonctions de sécurité et des mécanismes de sécurité en fonction des menaces et des risques. La section 2.6 traite du concept de la valeur de l'information numérique afin d'assurer un niveau de protection adéquat de celle-ci.

2.7.2.1 Les domaines de confiance

Tel qu'indiqué dans la section précédente, un domaine de confiance est défini comme un ensemble d'éléments d'ordre juridique, humain, organisationnel et technologique, un cadre de gestion de la sécurité, et un ensemble d'activités pertinentes à la sécurité qui sont tous assujettis à une politique de sécurité administrée par une seule autorité en matière de sécurité.

Au sens large, un domaine de confiance est composé d'un ensemble délimité de sujets authentifiés et d'objets devant être protégés auxquels s'applique une même politique de sécurité placée sous une autorité

commune[84]. Un domaine de confiance est donc un ensemble de ressources informatiques et de personnes ayant un niveau de sécurité interne homogène, appliquant la même politique de sécurité et représentant une entité autonome sur le plan de la sécurité.

Un domaine de confiance du gouvernement du Québec peut correspondre à un M/O ou une organisation responsable d'un secteur[85], d'une grappe de services ou d'un service gouvernemental au niveau des infrastructures commune et de la gouvernance[86] (politiques, directives, normes, etc.). Les domaines de confiance externes correspondent à des entités qui échangent des informations numériques ou encore qui transigent électroniquement avec l'appareil gouvernemental québécois mais qui ne sont pas sous sa gouvernance.

Pour les domaines de confiance sous la gouvernance de l'État, la politique de sécurité d'un domaine de confiance est définie par le sous-ministre ou le dirigeant d'organisme ou son représentant afin de s'assurer du respect des lois, ainsi que des objectifs, directives et normes de sécurité déterminés par le Conseil du trésor. Le sous-ministre ou le dirigeant d'organisme ou son représentant voit à ce que soit gérée la sécurité de l'information numérique tout au long de son cycle de vie. La politique de sécurité est un ensemble de mesures systématiques assurant la sécurité: rôles, responsabilités, dispositifs, règles, etc.

Une politique de sécurité a pour objectif d'apporter une orientation et un soutien de la part de la haute direction à la sécurité de l'information numérique. Il convient que la haute direction définisse clairement l'orientation de la politique et démontre son soutien et son engagement en ce qui concerne la sécurité de l'information numérique en diffusant et en mettant en oeuvre sa politique de sécurité dans toute l'organisation.

Le « Manuel canadien de la sécurité des technologies de l'information » discute de l'importance d'une politique de sécurité et propose un ensemble de sujets qui doivent être inclus dans une telle politique. Les intervenants oeuvrant dans le domaine de la sécurité peuvent s'inspirer de cette référence dans l'élaboration de leur politique de sécurité[87].

La norme ISO/IEC 17799 fournit des standards de contrôle des différents domaines informatiques, par exemple la politique de sécurité, l'organisation de la sécurité, la sécurité physique, la gestion des télécommunications et des systèmes et le contrôle des accès[88]. Les intervenants oeuvrant dans le domaine

[84] Historiquement, la délimitation d'un réseau a été d'abord de mettre en place un périmètre physique, mais cette délimitation est de plus en plus virtuelle. Un « domaine » comporte une idée de stabilité qui se trouve affectée par le caractère virtuel : on assistera en effet à une multiplication des domaines de confiance sous l'autorité gouvernementale, ce qui tendra à rapprocher le concept de celui d' « ententes de collaboration » qui caractérise le commerce électronique et où l'intersection entre domaines de confiance peut être minimal ou de brève durée, et où il n'y a pas d'autorité unique, mais plutôt deux parties prenantes ou plus qui collaborent sous des règles communes limitées à certains échanges.

[85] Les secteurs ou parties de secteur qui ne sont pas sous la gouverne de l'appareil gouvernemental sont traités comme un domaine de confiance externe.

[86] La gouvernance vise un développement économique, social et institutionnel durable, en maintenant un sain équilibre entre l'État, la société civile et le marché économique. Elle fait l'objet de plusieurs recommandations dans le cadre de l'AGSIN.

[87] On consultera le document *Manuel canadien de la sécurité des technologies de l'information* pour plus d'informations.

[88] On se référera à l'annexe D et à la norme ISO/IEC 17799 pour plus d'informations.

de la sécurité peuvent également s'inspirer de cette norme dans l'élaboration de leur politique de sécurité[89].

Chaque domaine de confiance sous la gouverne de l'État élabore un cadre de gestion de la sécurité en s'assurant de couvrir l'ensemble des dimensions de la sécurité tel que décrit à la section 2.4. La mise en oeuvre de la sécurité d'un domaine de confiance est à la charge notamment des responsables de la sécurité de l'information numérique (RSIN), des détenteurs, des responsables de la gestion documentaire et des responsables de l'accès à l'information et de la protection des renseignements personnels selon le contexte d'utilisation des processus d'affaires[90].

Les intervenants oeuvrant dans le domaine de la sécurité peuvent s'inspirer de la norme ISO/IEC 13335-2 qui établit un cadre permettant de spécifier la gestion et la planification de la sécurité des TI pour les systèmes ouverts dans l'élaboration de leur cadre de gestion de la sécurité[91] ainsi que du « Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise »[92].

De plus, le « Manuel canadien de la sécurité des technologies de l'information »[93] vise à fournir un aperçu global des aspects liés à la sécurité des TI afin de comprendre les besoins dans ce domaine et à mettre au point un mode judicieux de sélection des mesures appropriées de protection des TI. Le manuel ne contient aucune description détaillée des étapes de la mise en oeuvre d'un programme de sécurité, aucun procédé détaillé de mise en oeuvre des mesures de protection, ni aucun conseil relatif à la vérification de la sécurité de systèmes déterminés. Cependant, on trouvera ce genre de détails dans les publications mentionnées à la fin de chaque chapitre. Les intervenants oeuvrant dans le domaine de la sécurité peuvent s'inspirer de ces références dans l'élaboration du cadre de gestion de la sécurité[94].

La détermination de la valeur de l'information numérique dépend du contexte d'utilisation des processus d'affaires et du niveau de la catégorisation pour assurer un niveau acceptable de sécurité[95]. La détermination de la valeur de l'information numérique assurera une cohérence entre les domaines de confiance et avec les clientèles lors de l'élaboration des ententes et des interfaces sécuritaires.

À l'intérieur d'un domaine de confiance, les informations numériques doivent être protégées au niveau adéquat par des fonctions de sécurité. La détermination des mécanismes de sécurité supportant les fonctions de sécurité ainsi que des solutions technologiques nécessaires dépendra entre autres de la valeur des informations numériques à protéger ainsi que des menaces et des risques associés tel que présenté dans la section 2.6.

[89] Afin d'uniformiser l'élaboration d'une politique de sécurité et de préparer un guide d'utilisation, des travaux additionnels sont nécessaires au SCT.
[90] On consultera le document *Sécurité de l'information numérique, Receuil des pratiques recommandées, Partie 1 – Gestion de la sécurité* du SCT pour plus d'informations.
[91] On se référera à l'annexe D et à la norme ISO/IEC 13335-2 pour plus d'informations.
[92] On consultera le document *Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise* (février 2001) basée sur la norme ISO/IEC 13335 produit par le SCT pour plus d'informations.
[93] On consultera le document *Manuel canadien de la sécurité des technologies de l'information* pour plus d'informations.
[94] Afin d'uniformiser l'élaboration d'un cadre de gestion de la sécurité et de préparer un guide d'utilisation, des travaux additionnels sont nécessaires au SCT.
[95] On consultera le *Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité* pour plus d'informations.

Lorsque les informations numériques transitent dans un domaine de confiance ayant des mesures de protection de niveau inférieur, des mesures spéciales doivent être mises en oeuvre pour assurer le niveau adéquat de sécurité.

Les modalités d'affaires relatives aux interactions entre les domaines de confiance et avec les clientèles sont adressées dans les ententes. La section suivante présente le concept d'entente.

2.7.2.2 Ententes

Une entente définit les règles qui régissent les interactions entre les domaines de confiance ainsi qu'avec les clientèles. Elle permet également de délimiter les champs de compétence entre les domaines de confiance. Une entente contient au minimum une Interface sécuritaire. Il s'agit d'une forme d'accord ou de contrat entre un domaine de confiance et :

- un ou plusieurs autres domaine(s) de confiance;
- une ou plusieurs clientèle(s).

La rédaction de ces ententes est à la charge des détenteurs de systèmes d'information. Ces derniers pourront s'alimenter de diverses sources dont notamment les responsables de la sécurité de l'information numérique (RSIN), les responsables de la gestion documentaire et les responsables de l'accès à l'information et de la protection des renseignements et de toutes autres ressources jugées appropriées. Il doivent notamment définir[96] :

- les droits d'accès aux informations numériques;
- les responsabilités à l'égard de l'usage des informations numériques;
- les responsabilités pour la sauvegarde des informations numériques;
- les consentements nécessaires (explicite, libre, éclairé, spécifique et limité dans le temps);
- les limites de transfert des parties des informations numériques;
- l'engagement des parties à respecter les mesures de sécurité décrites dans les interfaces sécuritaires;
- l'engagement à accepter les audits ou les vérifications sur les incidents de sécurité relatives aux informations numériques;
- les dispositions garantissant le respect des exigences de sécurité comportant les éléments obligatoires déterminés par le Conseil du trésor;
- les conditions spéciales attachées aux informations numériques comme le respect de législations ou de règlements, notamment la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q c. A-2.1);
- toutes autres dispositions jugées pertinentes dans le respect des lois, des règlements, des directives, etc.

Les technicalités relatives aux interactions entre les domaines de confiance et avec les clientèles sont décrites dans les interfaces sécuritaires. La section suivante présente le concept d'interface sécuritaire.

[96] Afin d'uniformiser la détermination d'une entente et de préparer un guide d'utilisation, des travaux additionnels sont nécessaires au SCT.

2.7.2.3 Interface sécuritaire

Tel que défini dans la section 2.7.2, une interface sécuritaire définit les modalités techniques de sécurisation de l'information numérique. Elle est un ensemble d'éléments, comprenant à la fois des aspects logiciels et matériels, qui présente les normes et les fonctions de sécurité nécessaires pour assurer la connectivité et l'interopérabilité entre les domaines de confiance ainsi qu'avec les clientèles.

L'AGSIN propose les fonctions de sécurité, les mécanismes de sécurité et les solutions technologiques nécessaires pour assurer un niveau adéquat de sécurité de l'information numérique tout au long de son cycle de vie tel que présenté dans les sections 2.5 et 2.6.

Tel que mentionné à la section 2.7.2, l'AGSIN ne présuppose pas l'utilisation de produits particuliers en matière de sécurité mais propose des mécanises de sécurité et des solutions technologiques conformes aux normes et standards et ayant fait leurs preuves dans l'industrie afin d'assurer les fonctions de sécurité. Les critères pour le choix de produits particuliers qui supporteront les ÉÉ protégés doivent être déterminés[97]. Ce choix sera également influencé par la mise en commun, le partage ou la réutilisation potentielle des mécanismes de sécurité et des solutions technologiques nécessaires.

La protection de l'information numérique est basée sur les fonctions de sécurité suivantes :

- Intégrité;
- Irrévocabilité;
- Identification/authentification;
- Habilitation/contrôle d'accès;
- Confidentialité;
- Disponibilité;
- Surveillance;
- Administration.

Afin de déterminer une interface sécuritaire, un minimum d'éléments doivent être précisés. La définition des interfaces sécuritaires est sous la responsabilité des détenteurs de systèmes d'information. Ces derniers pourront s'alimenter de diverses sources dont notamment les responsables de la sécurité de l'information numérique (RSIN), les responsables de la gestion documentaire et les responsables de l'accès à l'information et de la protection des renseignements et de toutes autres ressources jugées appropriées (ex. : architectes technologiques et en sécurité). Les éléments devant être précisés incluent notamment :

- L'objet et la description de l'interface sécuritaire;
- La valeur des informations numériques;
- Les normes et standards de sécurité;
- Les fonctions et mécanismes de sécurité;
- Les solutions technologiques;
- Les règles de sécurité;

[97] On se référera à la section 2.4.4.2 pour plus de détails sur les critères pour le choix de produits.

- Autres éléments pertinents.

Le tableau suivant présente un certain nombre d'éléments à considérer appuyé d'un exemple afin de faciliter la détermination d'une interface sécuritaire[98].

Objet et description de l'interface sécuritaire	
Description	Exemple
• Déterminer l'objet de l'interface sécuritaire et fournir une brève description de son utilité	• Objet : transferts de fichiers en lots • Description : Cette interface sécuritaire vise l'échange électronique sécuritaire d'informations numériques entre domaines de confiance
Valeur des informations numériques (catégorisation)	
Description	Exemple
• Indiquer les niveaux de sécurité répertoriés sur les attributs de sécurité DICAI applicables pour assurer une sécurité adéquate ainsi que le contexte d'utilisation (poste autonome ou mobile, un réseau fermé ou un réseau ouvert).	• Disponibilité : basse • Intégrité : élevée • Confidentialité élevée • Authentification : moyenne • Irrévocabilité : N/A • (Serveur de transfert de fichiers accessibles sur réseau ouvert)
Normes et standards de sécurité	
Description	Exemple
• Identifier les normes et standards de sécurité pertinents	• ISO/IEC 10181-2, 3 et 6 • Commun Criteria EAL3 (ITSEC E2 ou TCSEC C2) • ISO/IEC 15408 • ISO/IEC 13335 • Internet , RFC 1421
Fonctions et mécanismes de sécurité	
Description	Exemple
• Identifier les fonctions de sécurité requises ainsi que les mécanismes sous-jacents	• Intégrité : Hachage (MD5) • Identification/authentification : Code d'usager et mot de passe • Habilitation/contrôle d'accès : Application FTP et coupe-feu • Confidentialité : chiffrement des données (DES en mode CBC)
Solutions technologiques	
Description	Exemple
• Identifier les composantes ou solutions technologiques retenues	• Application maison développée à l'aide d'API (EntrustFile™ Toolkit) • Serveur FTP • Coupe-feu

[98] Afin d'uniformiser la détermination d'une interface sécuritaire et de préparer un guide d'utilisation, des travaux additionnels sont nécessaires au SCT.

Règles de sécurité	
Description	Exemple
• Identifier les règles de sécurité à mettre en place sur les solutions technologiques retenues	• Application maison : Accès via code d'usager et mot de passe • Serveur FTP : Service FTP avec Code d'usager et mot de passe et accès en écriture seulement au répertoire désigné • Coupe-feu : Accès entrant au protocole FTP à l'adresse du serveur destinataire et accès sortant FTP à l'adresse du serveur source
Autres	
Description	Exemple
• Autres éléments d'informations pertinents	• Diagrammes • Schémas

3. LES VUES SPÉCIFIQUES DE L'AGSIN (PERSPECTIVE PHYSIQUE)

Cette section présente les vues spécifiques de l'AGSIN. Ces vues permettent de présenter, selon les différents volets de l'AEG, les concepts du modèle général de l'AGSIN et d'identifier le potentiel de mise en commun, de partage et de réutilisation des ressources en matière de sécurité. Les quatre volets présentés dans cette section sont les suivants :

- Volet affaires;
- Volet information;
- Volet application;
- Volet infrastructure technologique.

Lorsque pertinent, chaque volet présente et discute les éléments suivants :

- Une vue d'ensemble de la sécurité en fonction du volet;
- Le potentiel de mise en commun, de partage et de réutilisation;
- Un exemple illustrant la vue.

L'environnement commun comprendra les composantes qui seront communes pour l'ensemble de la communauté gouvernementale. L'environnement partagé entre plusieurs M/O réunira les composantes propres à une grappe de services. Les composantes réutilisables pourront être celles développées par un M/O et pouvant être réutilisées par d'autres M/O.

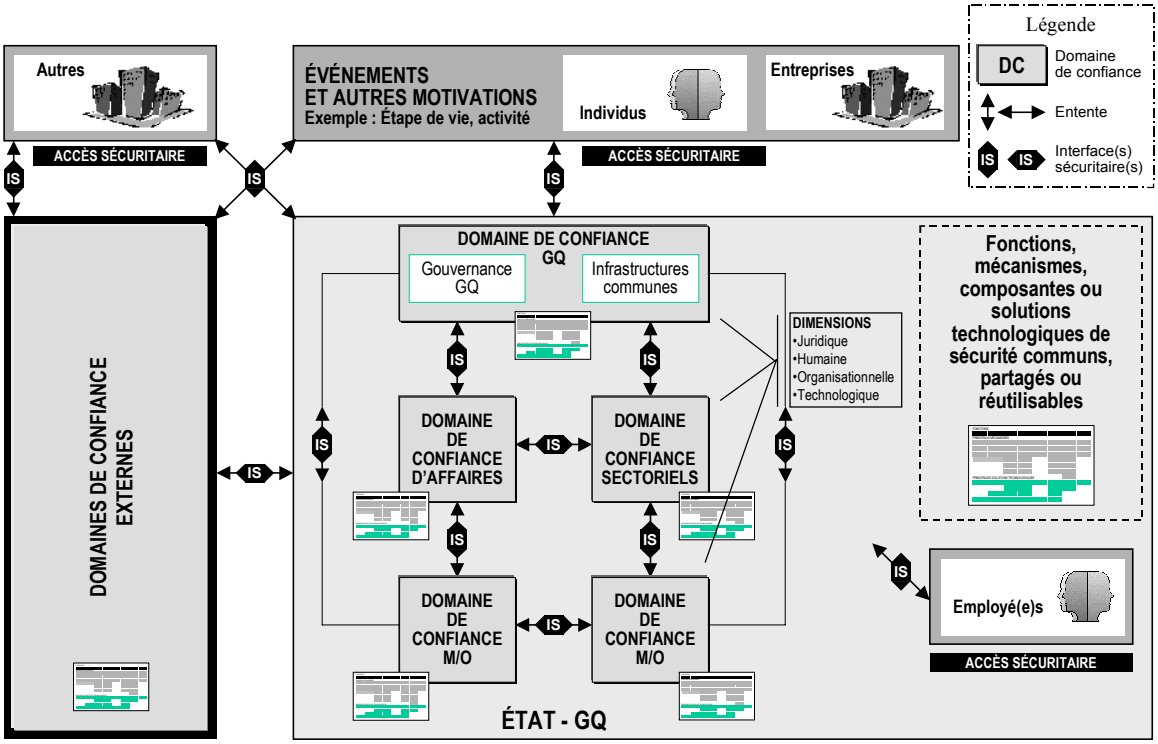
3.1 Volet affaires

Cette vue spécifique d'affaires de l'AGSIN présente les principaux concepts relatifs à la sécurité de l'information numérique (ces concepts viennent en complément aux concepts qui seront définis dans l'AEG).

3.1.1 La vue d'ensemble de la sécurité

La figure suivante illustre la vue affaires du modèle général de l'AGSIN ainsi que les concepts de domaine de confiance, d'entente et d'interface sécuritaire.

VUE AFFAIRES DU MODÈLE GÉNÉRAL DE L'AGSIN



La vue affaires du modèle général de l'AGSIN correspond en tout point au modèle général de l'AGSIN présenté à la section 2.7.2.

Bien qu'aucun détail supplémentaire ne sera livré ici, il est important de rappeler que le modèle général de l'AGSIN (et sa vue affaires) propose un certain nombre de concepts fondamentaux, présentés à la section 2.7 et aux sous sections 2.7.2.1 à 2.7.2.3, afin d'assurer une vision et une compréhension commune de la sécurité de l'information numérique par tous les intervenants impliqués au niveau de la sécurité de l'information numérique au sein de l'appareil gouvernemental. Ces concepts, soit les domaines de confiance, les ententes et les interfaces sécuritaires sont au cœur de l'AGSIN et se doivent d'être à la base des architectures de sécurité de l'information numérique des M/O et des organisations responsables d'un secteur, d'une grappe de services ou d'un service gouvernemental commun.

3.1.2 Potentiel de mise en commun, de partage ou de réutilisation

La vue affaires de l'AGSIN présente des potentiels intéressants de mise en commun, de partage et de réutilisation au niveau des ententes et des interfaces sécuritaires afin de créer un effet de levier simplifiant et accélérant le processus d'échange d'informations numériques sécuritaires. Certains processus d'affaires pourraient aussi être mis en commun, partagés ou réutilisés. Cette section présente les potentiels identifiés ainsi que le contexte d'utilisation.

Potentiel de mise en commun :

- Ententes et interfaces sécuritaires :
  - Une uniformisation de la façon dont les informations numériques sont échangées est possible au niveau :
    - des accès au répertoire gouvernemental des employé(e)s et aux certificats de clés publiques de chiffrement associés;
    - des accès au répertoire gouvernemental partenaires/mandataires et aux certificats de clés publiques de chiffrement associés;
    - des accès à l'ICPG pour la gestion des clés et des certificats ICPG des employé(e)s;
    - des accès à l'ICPG pour la gestion des clés et des certificats ICPG des mandataires/partenaires;
    - des accès à l'ICPG pour la gestion des clés et des certificats ICPG du pivot;
    - des accès (unifiés) au RICIB et au RETEM;
    - de l'utilisation des schémas XML de sécurité normalisés;
    - des accès (unifiés) aux applications gouvernementales et aux serveurs gouvernementaux;
    - des accès (unifiés) à GIRES;
    - des accès (unifiés) à l'intranet gouvernemental.
  - D'autres ententes et interfaces sécuritaires pourraient être uniformisées en fonction des besoins des M/O.
- Fonctions d'identification, d'authentification.

Potentiel de partage :

- Ententes et interfaces sécuritaires des secteurs de la santé, de l'Éducation et municipal :
  - Une uniformisation de la façon dont les informations numériques sont échangées est possible au niveau :
    - des accès (unifiés) aux applications sectorielles et aux serveurs sectoriels;
    - des accès (unifiés) aux réseaux sectoriels.
  - D'autres ententes et interfaces sécuritaires pourraient être uniformisées en fonction des services offerts par les secteurs de la santé, de l'Éducation et municipal .
- Ententes et interfaces sécuritaires élaborées par les organismes responsables d'une grappe de services :
  - Une uniformisation de la manière dont les informations numériques sont échangées est possible au niveau de diverses ententes et interfaces sécuritaires élaborées par les organisations responsables.

Potentiel de réutilisation :

- Ententes et interfaces sécuritaires des M/O;
  - Une uniformisation de la manière dont les informations numériques sont échangées est possible au niveau de diverses ententes et interfaces sécuritaires élaborées par les M/O.

3.1.3 Exemple

Afin d'aider à la compréhension des vues spécifiques et de leur utilité, un exemple de processus d'affaires électroniques est présenté[99]. Cet exemple sera utilisé à la fin de chaque vue spécifique afin d'illustrer l'utilisation de l'AGSIN dans l'élaboration des architectures de sécurité de l'information numérique spécifiques.

L'exemple utilisé consiste en un Extranet d'un M/O offrant aux entreprises abonnées, la possibilité de transmettre un formulaire électronique. Ainsi, un formulaire électronique est accessible à partir du serveur Web du site Extranet du M/O. Une fois complété, ce formulaire est chiffré afin d'assurer la confidentialité et signé numériquement afin d'assurer l'irrévocabilité par une personne habilitée de l'entreprise. Le formulaire est ensuite transmis au M/O et emmagasiné dans une base de données pour traitement ultérieur par une personne habilitée du M/O .

Cet exemple pose les hypothèses suivantes :

- la personne habilitée de l'entreprise possède un certificat de clé publique reconnu par l'ICPG;
- la personne habilitée du M/O a un certificat de clé publique émis à cet employé dans le cadre de l'ICPG.

Deux domaines de confiance gouvernementaux sont mis à contribution dans ce processus d'affaires électronique. Le domaine de confiance du M/O fournit les services spécifiques d'Extranet via un site Web offrant un formulaire électronique. Le domaine de confiance du GQ offre les services communs d'ICPG, de répertoire et de réseautage.

Chaque domaine de confiance doit s'assurer que les mesures de sécurité (politique de sécurité et cadre de gestion de la sécurité) respectent les orientations gouvernementales en matière de sécurité.

À priori, du point de vue affaires, des ententes et des interfaces sécuritaires sont requises dans ce processus d'affaires notamment pour assurer :

- L'utilisation sécuritaire des services Extranet par les entreprises au niveau du domaine de confiance du M/O;
- L'utilisation sécuritaire des services de l'ICPG au niveau du domaine de confiance du GQ par le domaine de confiance du M/O;
- L'utilisation sécuritaire des services de répertoire au niveau du domaine de confiance du GQ par le domaine de confiance du M/O;
- L'utilisation sécuritaire des services du RETEM au niveau du domaine de confiance du GQ par le domaine de confiance du M/O.

[99] L'exemple utilisé ne prétend pas couvrir tous les éléments à considérer dans l'élaboration d'une ASIN spécifique. Il se veut un complément aux vues spécifiques afin de présenter la manière dont s'articulent les concepts de sécurité avancés dans l'AGSIN.

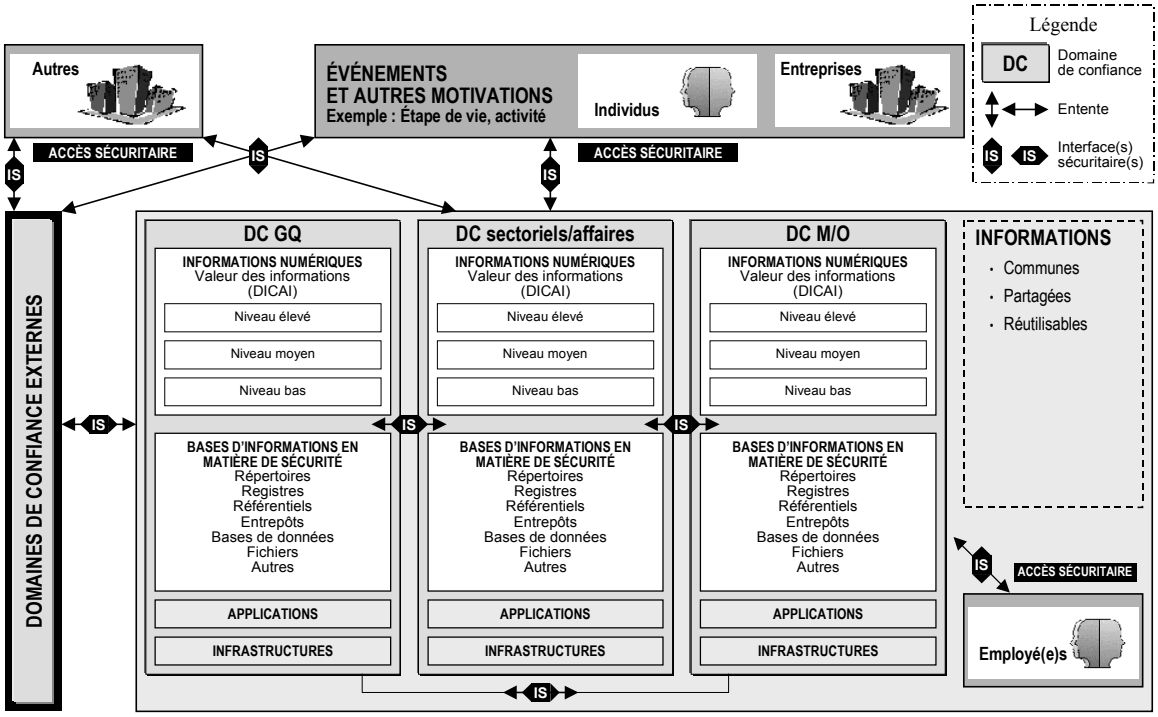
3.2 Volet information

Cette vue spécifique de l'information de l'AGSIN présente les principaux éléments d'information relatifs à la sécurité de l'information numérique (ces éléments d'information viennent en complément aux éléments d'information qui seront définis dans l'AEG). Les éléments d'information relatifs à l'AGSIN sont présentés plus en détails dans les pages suivantes.

3.2.1 La vue d'ensemble de la sécurité

La figure suivante illustre la vue information du modèle général de l'AGSIN ainsi que le concept de base d'informations en matière de sécurité.

VUE INFORMATION DU MODÈLE GÉNÉRAL DE L'AGSIN



Tel que nous l'avons vu précédemment, la valeur de l'information numérique est déterminée en fonction d'un certain nombre de paramètres. Le « Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité » définit trois niveaux de sécurité qui sont répertoriés sur les attributs de sécurité DICAI soit, sécurité basse, moyenne ou élevée. Afin de compléter la détermination de la valeur de l'information numérique, le contexte d'utilisation est également précisé[100].

[100] On se référera au *Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité* pour plus d'informations.

Afin d'assurer un niveau adéquat de sécurité en fonction de la valeur de l'information numérique, une base d'informations en matière de sécurité est nécessaire pour la gestion des mécanismes de sécurité et des solutions technologiques supportant les fonctions de sécurité. Ces informations en matière de sécurité possèdent une valeur élevée et nécessitent elles-mêmes des mécanismes de sécurité et solutions technologiques assurant un niveau élevé de sécurité.

La gestion de la sécurité de l'information numérique dans un monde ouvert et réparti peut imposer un grand nombre de politiques de sécurité et plusieurs cadres de gestion de la sécurité incluant des normes, des standards et de meilleures pratiques en cette matière. Par définition, les entités qui sont soumises à une politique de sécurité et administrées par une autorité en matière de sécurité se retrouvent dans un même domaine de confiance. Les domaines de confiance et leurs interactions sont à la base de l'AGSIN et de son évolution.

Tel que mentionné dans la section 2.7.2, chaque domaine de confiance définit sa propre politique de sécurité et élabore un cadre de gestion correspondant en s'assurant de couvrir l'ensemble des dimensions de la sécurité. Il est également mentionné dans la même section que la politique de sécurité est administrée par l'autorité en matière de sécurité du domaine de confiance.

La gestion des mécanismes de sécurité ainsi que des solutions technologiques nécessite la répartition d'informations de gestion dans ces mêmes mécanismes de sécurité et solutions technologiques ainsi que la collecte d'informations concernant leur fonctionnement.

La liste suivante énonce les principaux éléments d'information en matière de sécurité susceptibles d'être requis et utilisés dans les domaines de confiance :

- La politique de sécurité;
- Le cadre de gestion de la sécurité;
- Les informations d'identification/authentification des entités (et leur localisation);
- Les certificats de clés publiques de chiffrement (et leur localisation);
- Les profils d'habilitation/contrôle d'accès (et leur localisation);
- Les certificats d'attributs (et leur localisation);
- Les règles de surveillance et de définition des virus;
- Les règles de surveillance et de définition des intrusions réseau;
- Les règles de surveillance et de définition des intrusions serveur;
- Les règles de surveillance et de définition des intrusions SGBD;
- Les règles de surveillance et de définition de contenus actifs;
- Les règles de surveillance et de définition des accès des coupe-feu;
- Les règles de surveillance et de définition des accès et des routeurs;
- Les règles de paramétrisation et de sécurisation du matériel;
- Les règles de paramétrisation et de sécurisation des systèmes d'exploitation et des logiciels;
- Les métadonnées en matière de sécurité (documents, transactions, etc.);
- Etc.

Les éléments d'information qui sont relatifs à la sécurité de l'information numérique d'un domaine de confiance se retrouvent donc dans une base d'informations constituée d'un ensemble conceptuel d'informations en matière de sécurité nécessaires à l'administration et à la gestion de l'information numérique. La base d'informations en matière de sécurité d'un domaine de confiance est donc une base d'informations répartie ayant une valeur nécessitant un niveau approprié de sécurité.

La base d'information en matière de sécurité est principalement constituée des informations relatives à la gestion des informations numériques, des applications relatives à la sécurité et des infrastructures technologiques nécessaires à la sécurité. Elle peut donner lieu à la création de schémas, de tableaux, de fichiers, de données, de règles, etc. qui doivent être emmagasinés et échangés de manière sécuritaire. Les éléments de la base d'informations en matière de sécurité sont inclus notamment dans :

- Des répertoires ou annuaires :
  - Mécanisme d'entreposage pour des noms et adresses d'entités (personnes, applications) devant être associées à des certificats de clés publiques afin de garantir leur identification et leurs autorisations dans le fonctionnement normal et en sécurité des affaires.
- Des registres :
  - Mécanisme d'enregistrement d'objets institué par une organisation en vue de permettre à ses acteurs légitimes l'inscription de métadonnées identifiant et décrivant un objet ainsi que la localisation indiquant où est simultanément placé l'objet dans un lieu distinct d'entreposage (le référentiel)[101].
- Des référentiels :
  - Mécanisme d'entreposage, de préservation et de distribution des fichiers contenant les définitions de structures, soit les objets correspondant aux items inscrits dans un registre ou plus. Dans le modèle OASIS, le référentiel est une sorte d'entrepôt spécialisé pour les objets hautement réutilisables que sont les définitions de structures.
- Des entrepôts ou des bases de données :
  - Mécanisme commun d'entreposage, de préservation et de distribution de données physiques rassemblées pour des raisons d'aide à la décision, de sécurité, de traitement analytique, de préservation à long terme ou autre.
- Autres dépôts d'informations.

La base d'informations en matière de sécurité d'un domaine de confiance peut faire appel à des informations en matière de sécurité d'un ou de plusieurs autres domaines de confiance. Il faut donc accorder une attention particulière à la protection des échanges d'informations en matière de sécurité entre les domaines de confiance de façon à ne pas affaiblir le niveau de protection prévu.

À cet effet, des ententes et des interfaces sécuritaires particulières relatives à l'échange d'information entre les bases d'information en matière de sécurité sont nécessaires. À titre d'exemple, la certification réciproque entre deux autorités de certification exige un ensemble de mesures de protection très strictes.

[101] Registre évoque une autorité d'enregistrement, des statuts transitoires dans des procédures d'inscription, la classification et la validation des références conservées dans le registre aux fins de repérage par les utilisateurs et de contrôle par l'autorité d'enregistrement et les autorisations réparties de création et mise à jour parmi les propriétaires de processus d'affaires.

3.2.2 Potentiel de mise en commun, de partage ou de réutilisation

Les informations nécessaires au support des fonctions de sécurité assurées par les mécanismes de sécurité et les solutions technologiques peuvent être dédiées au DC ou être de nature commune, partagée ou réutilisable.

Plusieurs dépôts d'informations de la base d'informations en matière de sécurité ont un potentiel intéressant de mise en commun[102], de partage ou de réutilisation. Cette section présente les potentiels identifiés ainsi que le contexte d'utilisation[103].

Potentiel de mise en commun :

- Répertoire(s) gouvernemental(aux) des informations relatives aux employés et aux partenaires/mandataires et certificats de clés publiques de chiffrement associés :
  - L'information relative à l'identification et la localisation des employés et des mandataires/partenaires ainsi que des certificats de clés publiques de chiffrement associés a grand avantage à être facilement accessible afin de ne pas freiner les initiatives nécessitant les fonctions d'identification/authentification forte, d'intégrité et de confidentialité élevée et d'irrévocabilité.
  - D'autres informations en matière de sécurité de l'information numérique pourraient éventuellement être mises en commun.
- Base de données de GIRES des informations relatives aux employés et aux partenaires/mandataires :
  - L'information relative aux employés ainsi qu'aux partenaires/mandataires pourrait servir à alimenter les répertoires gouvernementaux des employés et des partenaires/mandataires
  - D'autres informations en matière de sécurité de l'information numérique pourraient éventuellement être tirées de GIRES.
- Base de données et fichiers des règles de sécurité du RICIB et du RETEM :
  - Le RICIB et le RETEM utilisent plusieurs dépôts contenant des informations en matière de sécurité qui ont un potentiel de mise en commun afin d'uniformiser l'administration de la sécurité et la surveillance de l'information numérique qui transite sur ce réseau. On retrouve notamment :
    - Les bases de données des règles de surveillance et de définition des virus;
    - Les bases de données des règles de surveillance et de définition des intrusions;
    - Les bases de données des règles de surveillance et de définition des accès des coupe-feu et des aiguilleurs.
  - D'autres de règles de surveillance et de définition pourraient également faire l'objet de mise en commun dépendamment des services de sécurité réseaux offerts par le RICIB et le RETEM.

Potentiel de partage :

[102] L'ICPG, le répertoire gouvernemental et GIRES sont déjà retenus comme infratructures communes par le SCT. Cependant, il reste des travaux afin de savoir qui, quoi, quand, comment, etc. sera mis en commun.

[103] Il est important de noter que chaque système peut contenir des informations locales en matière de sécurité nécessaires pour appliquer une politique de sécurité cohérente au sein du domaine de confiance.

- Registre-référentiel des schémas XML de sécurité normalisés :
  - Les modèles d'interopérabilité basés sur la norme XML sont très flexibles en ce qui a trait au degré possible de partage pour la réutilisation des métadonnées. Les travaux gouvernementaux[104] basés notamment sur le standard ebXML ont permis de modéliser un certaine nombre de schémas de metadonnées (composants noyaux) en matière de sécurité pouvant être partagés soit :
    - Profil de métadonnées;
    - Tableau des autorisations;
    - Étiquette de signature numérique;
    - Circuit de production (workflow).
  - D'autres schémas de métadonnées en matière de sécurité seront éventuellement modélisés et partageables[105].
- Base de données et fichiers des règles de sécurité des réseaux des secteurs de la santé et de l'Éducation.
  - Les réseaux sectoriels utilisent plusieurs dépôts contenant des informations en matière de sécurité qui ont un potentiel de partage afin d'uniformiser l'administration de la sécurité et la surveillance de l'information numérique qui transite sur ces réseaux. On retrouve notamment :
    - Les bases de données des règles de surveillance et de définition des virus;
    - Les bases de données des règles de surveillance et de définition des intrusions;
    - Les bases de données des règles de surveillance et de définition des accès des coupe-feu;
    - Les bases de données des règles de surveillance et de définition des accès des aiguilleurs.
  - D'autres dépôts de règles de surveillance et de définition pourraient également faire l'objet de partage dépendamment des services de sécurité réseaux offerts par les réseaux sectoriels.
- Registres-référentiels particuliers XML des secteurs ou grappes;
- Bases de données des règles de sécurité des secteurs ou grappes.

Potentiel de réutilisation :

- Registres-référentiels particuliers XML des M/O;
- Bases de données des règles de sécurité des M/O :
  - Les M/O utilisent plusieurs dépôts contenant des informations en matière de sécurité pouvant être réutilisées afin d'uniformiser l'administration de la sécurité et la surveillance de l'information numérique entre eux. On retrouve notamment :
    - Les bases de données des règles de surveillance et de définition des virus;
    - Les bases de données des règles de surveillance et de définition des intrusions;
    - Les bases de données des règles de surveillance et de définition des accès des coupe-feu;
    - Les bases de données des règles de surveillance et de définition des accès des aiguilleurs.

[104] On consultera le document *XML en route au gouvernement du Québec* http://www.autoroute.gouv.qc.ca/publica/xml.pdf pour plus d'informations.
[105] On se référera à l'hyperlien http://www.autoroute.gouv.qc.ca/publica/pub_ingenerie.htm pour plus d'informations.

- D'autres dépôts de règles de surveillance et de définition pourraient également faire l'objet de réutilisation entre les M/O;

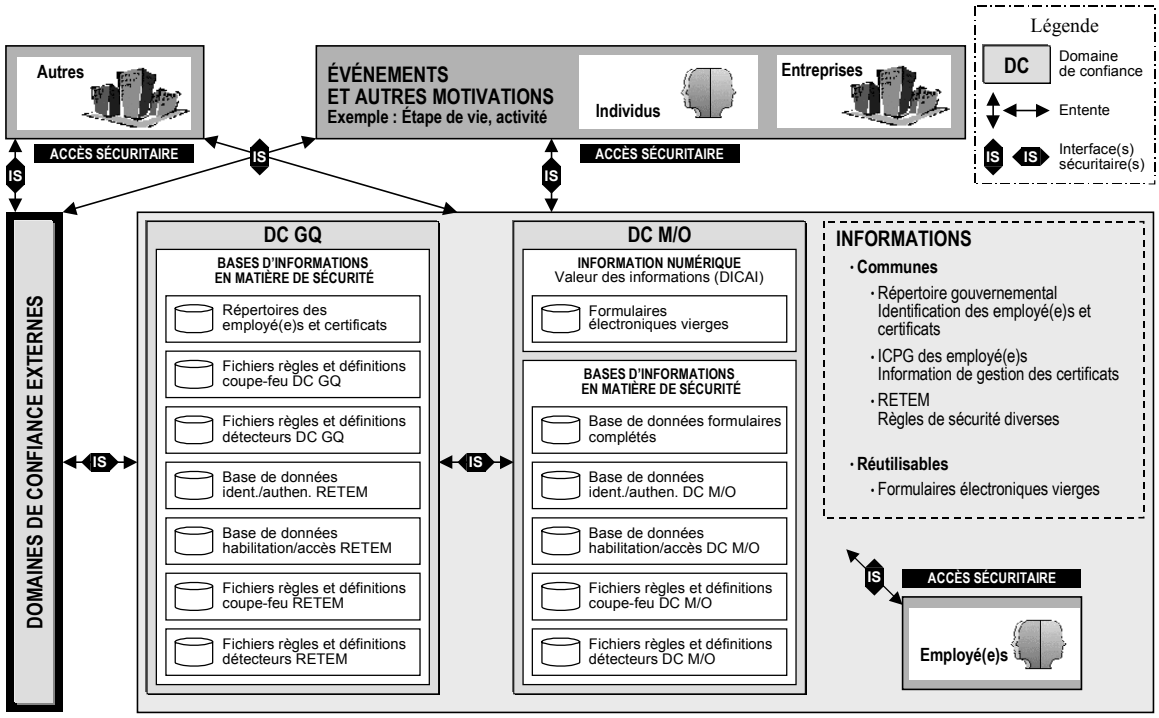
- Formulaires électroniques vierges.

3.2.3 Exemple

Dans l'exemple de l'Extranet d'un M/O offrant aux entreprises abonnées la possibilité de transmettre un formulaire électronique, plusieurs dépôts d'informations sont mis à contribution. On retrouve ainsi dans chaque domaine de confiance un ensemble de dépôts d'informations répartis afin d'assurer la sécurité du processus d'affaires électroniques.

La figure suivante illustre les principaux dépôts d'informations de la base d'informations en matière de sécurité de chaque domaine de confiance mis à contribution.

PRINCIPAUX DÉPÔTS D'INFORMATIONS DE LA BASE D'INFORMATIONS EN MATIÈRE DE SÉCURITÉ



Sans être exhaustive, la liste des dépôts d'informations donne une bonne idée des informations nécessaires afin d'assurer la sécurité du processus d'affaires électroniques. Ces informations doivent être hautement protégées afin de ne pas compromettre la sécurité de chaque domaine de confiance. Il est de la responsabilité de chaque domaine de confiance de protéger adéquatement les informations de la base d'informations en matière de sécurité selon leur politique de sécurité et leur cadre de gestion de sécurité respectifs.

Le registre-référentiel du domaine de confiance du M/O est une composante déterminante du processus d'affaires électroniques. En effet, il contient notamment le formulaire vierge qui est en fait un document abstrait offrant une structure logique (intégrant les schémas de sécurité) et graphique. Une fois rempli par la personne habilitée de l'entreprise, le formulaire complété devient un document concret de la base de données des formulaires complétés.

Au niveau du domaine de confiance du M/O, un exercice de catégorisation de l'information numérique contenue dans le formulaire permet de définir la valeur de l'information en fonction des attributs (fonctions) de DICAI (et des fonctions d'habilitation/contrôle d'accès, de surveillance et d'administration) et par la suite de définir les mécanismes de sécurité et les solutions technologiques appropriés.

Aussi chaque domaine de confiance s'assurera que des ententes et des interfaces sécuritaires appropriées existent pour l'échange d'informations entre les bases d'informations en matière de sécurité et pour l'utilisation des formulaires électroniques.

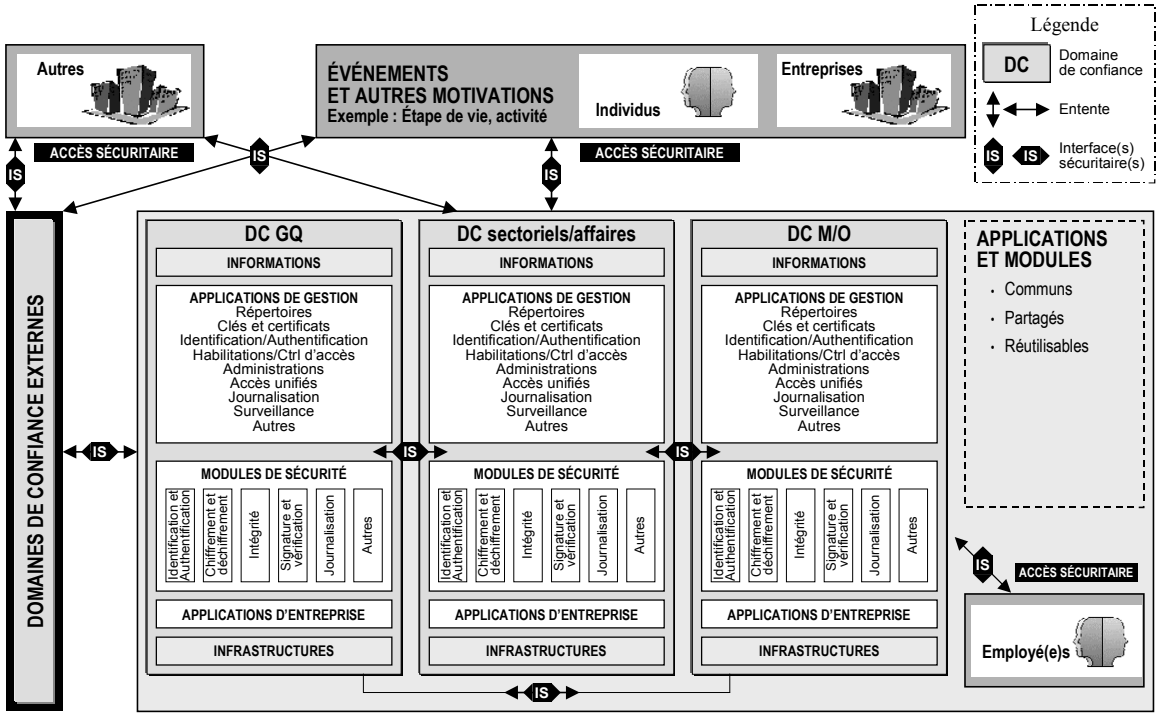
3.3 Volet application

Cette vue spécifique des applications de l'AGSIN présente les principales applications relatives à la sécurité ainsi que les modules de sécurité supportant la sécurité de l'information numérique (ces éléments d'application viennent en complément aux éléments d'application qui seront définis dans l'AEG). Les éléments d'application relatifs à l'AGSIN sont présentés en détails dans les pages suivantes.

3.3.1 La vue d'ensemble de la sécurité

La figure suivante illustre la vue application du modèle général de l'AGSIN ainsi que les concepts d'application relative à la gestion de la sécurité et de module de sécurité.

VUE APPLICATION DU MODÈLE GÉNÉRAL DE L'AGSIN



Les applications relatives à la gestion de la sécurité ainsi que les modules supportant la sécurité favorisent une vision commune de l'environnement applicatif de sécurité.

La base d'information en matière de sécurité requiert une gestion adaptée à la valeur des informations qu'elle contient. À cet effet, chaque domaine de confiance doit mettre en place des applications relatives à la gestion de la sécurité. La base d'information en matière de sécurité étant répartie, les domaines de confiance doivent sélectionner et/ou développer des produits facilitant une gestion centralisée de ces informations.

Les applications relatives à la gestion de la sécurité traitent donc de la gestion des mécanismes de sécurité et des solutions technologiques assurant les fonctions de sécurité. Ces applications doivent être conformes aux normes et standards et, lorsque pertinent, avoir fait leurs preuves dans l'industrie et être certifiées par des organismes reconnus tel que présenté à la section 2.4.4.2.

Dans le cas d'acquisition d'applications relatives à la gestion de la sécurité, les critères de sélection de produits particuliers devront être déterminés[106] de manière précise afin d'assurer au maximum l'interopérabilité des produits. Ce choix sera de plus influencé par la mise en commun, le partage ou la réutilisation potentielle des mécanismes de sécurité et des solutions technologiques.

Dans le cas où des applications relatives à la gestion de la sécurité doivent être développées, les normes et standards de développement strictes en matière de sécurité devront être précisées dans la cadre de développement tel que présenté à la section 2.4.4.1.

Dans les deux cas, des intervenants spécialisés de divers domaines seront impliqués ou consultés lors de l'acquisition ou du développement d'applications relatives à la gestion de la sécurité.

La liste suivante présente les principales applications relatives à la gestion de la sécurité retenues dans le cadre de l'AGSIN. Cette liste n'est pas exhaustive et peut varier en fonction notamment des besoins spécifiques de l'État, des nouveaux besoins gouvernementaux ou des technologies émergentes.

- Gestion des répertoires :
  - Les aspects de la gestion des répertoires concernent principalement la définition, l'administration et la répartition des classes d'objet.
- Gestion des clés et des certificats :
  - Les aspects de la gestion des clés et des certificats concernent principalement la définition, l'administration et la répartition des clés et des certificats durant tout leur cycle de vie.
- Gestion des habilitations/contrôles d'accès :
  - Les aspects de la gestion des habilitations/contrôles d'accès concernent principalement la définition, l'administration et la répartition des attributs de sécurité (profils, certificats d'attributs), des listes de contrôle d'accès et des règles d'accès, etc. La gestion de l'habilitations/contrôle d'accès est étroitement liée à la gestion des accès unifiés.
- Gestion de l'administration :
  - Les aspects de la gestion de l'administration concernent principalement l'installation, la paramétrisation et la sécurisation des logiciels, du matériel et des équipements de réseautage.

[106] On consultera la section 2.4.4.2 pour plus de détails sur les critères de sélection des applications.

- Gestion des accès (unifiés) :
  - Les aspects de la gestion des accès (unifiés) concernent principalement la définition, l'administration et la répartition des identifiants et des authentifiants. La gestion des accès unifiés est étroitement liée à la gestion des habilitations/contrôles d'accès.
- Gestion de la journalisation :
  - Les aspects de la gestion de la journalisation concernent principalement le traitement des notifications et des événements de déclenchement des notifications. La gestion de la journalisation est étroitement liée à la gestion de la surveillance.
- Gestion de la surveillance :
  - Les aspects de la gestion de la surveillance concernent le choix d'événement à enregistrer et la préparation de rapports d'audits. La gestion de la surveillance est étroitement liée à la gestion de la journalisation.
- Autres :
  - Toute autre application relative à la gestion de la sécurité pertinente en fonction des besoins.

Tel que présenté dans la vue application du modèle général de l'AGSIN, l'AGSIN préconise une sécurité modulaire favorisant un découpage entre les fonctions de traitement des applications d'entreprises et les fonctions de sécurité afin d'assurer un maximum de flexibilité et d'interopérabilité. Ce découpage favorise également la mise en commun, le partage et la réutilisation de modules de sécurité.

Les modules de sécurité visent à fournir les fonctions de sécurité aux applications d'entreprise. Ils utilisent principalement les informations en matière de sécurité gérées par les applications relatives à la gestion de la sécurité.

Comme c'est le cas lors de l'acquisition d'applications relatives à la gestion de la sécurité, des critères de sélection de produits particuliers devront être déterminés de manière précise pour le choix des modules et ce dernier sera de plus influencé par la mise en commun, le partage ou la réutilisation potentielle des produits.

Dans le cas de développement de modules supportant la sécurité, des normes et standards de développement strictes en matière de sécurité devront être précisées dans le cadre de développement.

Dans ces deux cas, des intervenants spécialisés de divers domaines seront impliqués ou consultés dans le processus d'acquisition ou de développement.

Les principaux modules nécessaires à la sécurité de l'information numérique identifiés dans le cadre de l'AGSIN incluent :

- Identification et authentification :
  - Ces modules peuvent être des composants commerciaux ou maison, des plugiciels, des DLL, etc. qui sont utilisés par les applications d'entreprises afin d'assurer la fonction d'identification/authentification.
- Habilitation et contrôle d'accès :
  - Ces modules peuvent être des composants commerciaux ou maison, des plugiciels, des DLL, etc. qui sont utilisés par les applications d'entreprises afin d'assurer la fonction d'habilitation/contrôle d'accès.
- Chiffrement et déchiffrement :

  - Ces modules peuvent être des composants commerciaux ou maison, des plugiciels, des DLL, etc. qui sont utilisés par les applications d'entreprises afin d'assurer la fonction de confidentialité.
- Intégrité :
  - Ces modules peuvent être des composants commerciaux ou maison, des plugiciels, des DLL, etc. qui sont utilisés par les applications d'entreprises afin d'assurer la fonction d'intégrité.
- Signature et vérification :
  - Ces modules peuvent être des composants commerciaux ou maison, des plugiciels, des DLL, etc. qui sont utilisés par les applications d'entreprises afin d'assurer la fonction d'irrévocabilité.
- Journalisation :
  - Ces modules peuvent être des composants commerciaux ou maison, des plugiciels, des DLL, etc. qui sont utilisés par les applications d'entreprises afin d'assurer la fonction d'irrévocabilité.
- Autres.

Comme dans le cas des applications relatives à la gestion de la sécurité, la liste des modules n'est pas exhaustive et peut varier en fonction notamment des besoins spécifiques de l'État, des nouveaux besoins gouvernementaux ou des technologies émergentes.

3.3.2 Potentiel de mise en commun, de partage ou de réutilisation

Les applications relatives à la gestion de la sécurité et les modules de sécurité nécessaires au support des fonctions de sécurité peuvent être dédiés au DC ou être de nature commune, partagée ou réutilisable.

Plusieurs applications relatives à la gestion de la sécurité et modules de sécurité ont un potentiel intéressant de mise en commun[107], de partage ou de réutilisation. Cette section présente les applications relatives à la gestion de la sécurité et les modules de sécurité pouvant potentiellement être mis en commun, partagés ou réutilisés, ainsi que leur contexte d'utilisation.

Potentiel de mise en commun :

- Les applications relatives à la gestion de la sécurité et les modules de sécurité:
  - Plusieurs applications relatives à la gestion de la sécurité et modules de sécurité pourraient éventuellement être mises en commun (ou le sont déjà) afin de faciliter l'administration de la sécurité et la surveillance. Ces applications et modules comprennent :
    - Application(s) de gestion du répertoire gouvernemental des employé(e)s;
    - Application(s) de gestion du répertoire gouvernemental des mandataires/partenaires;
    - Application(s) de gestion des clés et des certificats ICPG des employé(e)s;
    - Application(s) de gestion des clés et des certificats ICPG des mandataires/partenaires;
    - Application(s) de gestion des clés et des certificats ICPG du pivot;
    - Application(s) de gestion de l'administration du RICIB et du RETEM;
    - Application(s) de gestion de la journalisation du RICIB et du RETEM;

[107] L'ICPG, le répertoire gouvernemental et GIRES sont déjà retenus comme infratructures communes par le SCT. Cependant, il reste des travaux afin de savoir qui, quoi, quand, comment, etc. sera mis en commun.

- Application(s) de gestion de la surveillance du RICIB et du RETEM;
- Module(s) d'identification et d'authentification;
- Module(s) de chiffrement et déchiffrement.
- Application(s) de gestion de l'administration des applications gouvernementales et des serveurs gouvernementaux;
- Application(s) de gestion de la journalisation des applications gouvernementales et des serveurs gouvernementaux;
- Application(s) de gestion de la surveillance des applications gouvernementales et des serveurs gouvernementaux;
- Application(s) de gestion des accès (unifiés) des applications gouvernementales et des serveurs gouvernementaux;
- Module(s) de signature et de vérification;
- Module(s) de journalisation;

➢ D'autres applications relatives à la gestion de la sécurité et modules de sécurité pourraient être mises en commun dépendamment des orientations gouvernementales.

Potentiel de partage :

- Les applications relatives à la gestion de la sécurité et les modules de sécurité des secteurs de la santé, de l'Éducation et municipal :
  - ➢ Plusieurs applications relatives à la gestion de la sécurité et modules de sécurité de ces secteurs pourraient éventuellement être partagées afin de faciliter l'administration de la sécurité et la surveillance. Ces applications et modules comprennent :
    - Application(s) de gestion de l'administration des réseaux sectoriels;
    - Application(s) de gestion de la journalisation des réseaux sectoriels;
    - Application(s) de gestion de la surveillance des réseaux sectoriels;
    - Module(s) d'identification et d'authentification;
    - Module(s) de chiffrement et déchiffrement;
  - ➢ D'autres applications relatives à la gestion de la sécurité et modules de sécurité de ces secteurs pourraient être partagées dépendamment des orientations de ceux-ci.

➢ Applications et modules de sécurité propres à une grappe.

Potentiel de réutilisation :

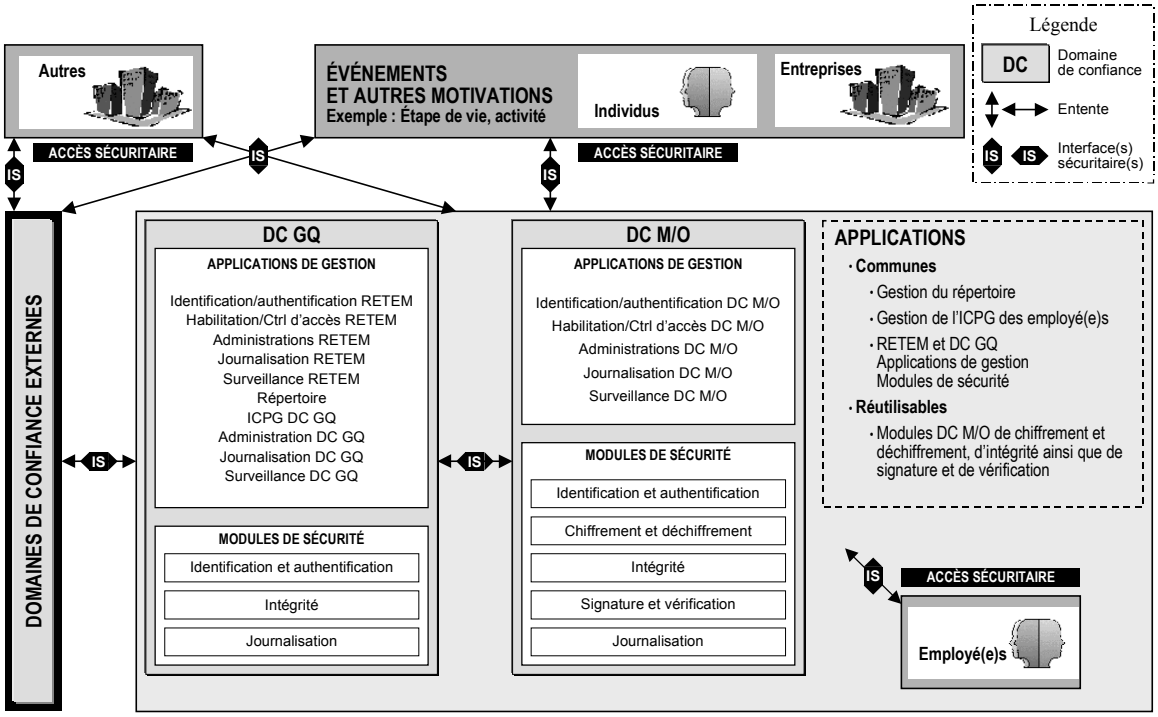
- Plusieurs modules de sécurité des M/O pourraient être réutilisés afin de faciliter et d'uniformiser les échanges d'information numériques sécuritaires entre les domaines de confiance et avec les clientèles.
  - ➢ Module(s) de journalisation d'un M/O;
  - ➢ Module(s) de vérification d'intégrité d'un M/O;
  - ➢ Etc.

3.3.3 Exemple

Toujours selon le même exemple de l'Extranet d'un M/O offrant aux entreprises abonnées la possibilité de transmettre un formulaire électronique, les bases d'informations en matière de sécurité des domaines de confiance doivent être gérées adéquatement afin de s'assurer que les mécanismes de sécurité et les solutions technologiques supportant les fonctions de sécurité requises répondent aux besoins de sécurité du processus d'affaires électroniques.

La figure suivante illustre les principales applications relatives à la gestion de la sécurité et les principaux modules de sécurité de chaque domaine de confiance requis.

PRINCIPALES APPLICATIONS RELATIVES À LA GESTION DE LA SÉCURITÉ ET MODULES DE SÉCURITÉ REQUIS



À prime abord, la liste des applications relatives à la gestion de la sécurité et des modules de sécurité identifiés pour chaque M/O n'est pas exhaustive. Elle illustre cependant très bien ceux qui sont nécessaires pour supporter le processus d'affaires électroniques.

Ainsi chaque domaine de confiance voit à ce que les applications relatives à la gestion de la sécurité sous sa responsabilité soient gérées en conformité avec la politique de sécurité et le cadre de gestion de sécurité. Chaque domaine de confiance voit également à ce que l'intégration des modules de sécurité soit effectuée de manière sécuritaire.

3.4 Volet infrastructure technologique

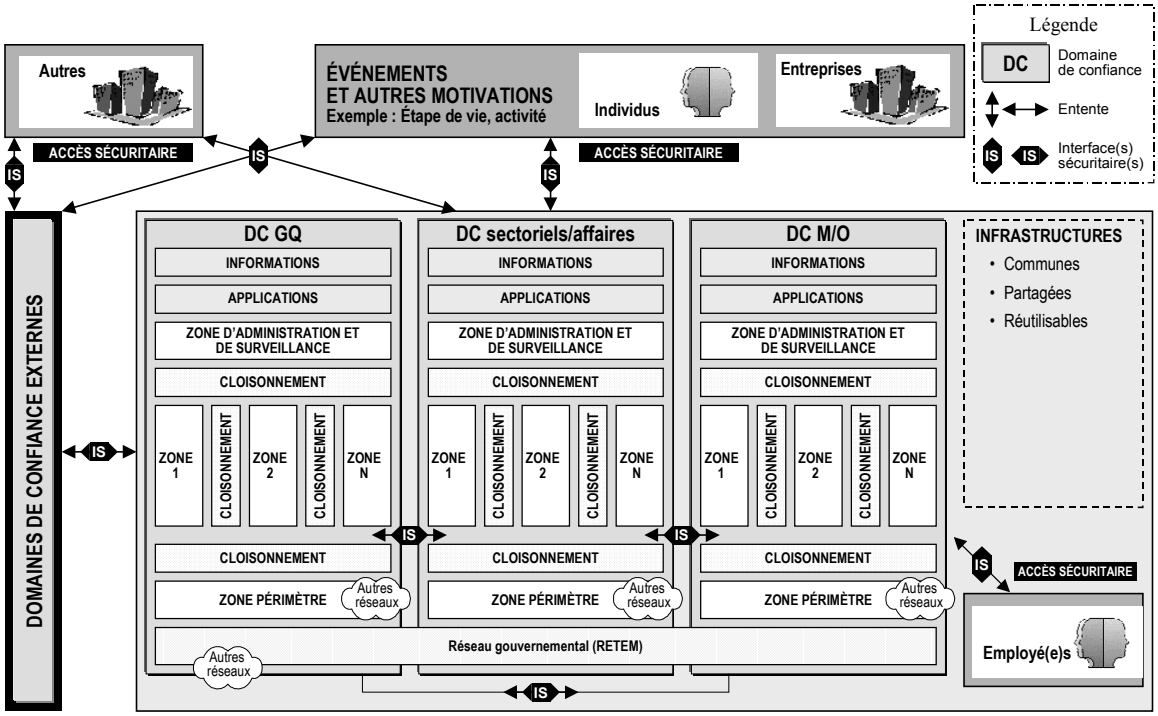
Cette vue spécifique de l'infrastructure technologique de l'AGSIN présente les principales infrastructures technologiques relatives à la sécurité de l'information numérique (ces éléments d'infrastructure technologique viennent en complément aux éléments d'infrastructure technologique qui seront définis

dans l'AEG). Les éléments d'infrastructure technologique relatifs à l 'AGSIN sont présentés dans les pages suivantes.

3.4.1 La vue d'ensemble de la sécurité

La figure suivante illustre la vue infrastructure technologique du modèle général de l'AGSIN ainsi que les concepts de cloisonnement et de zone. De plus, elle positionne le réseau gouvernemental (RETEM).

VUE INFRASTRUCTURE TECHNOLOGIQUE DU MODÈLE GÉNÉRAL DE L'AGSIN



Cette vue spécifique de l'infrastructure technologique de l'AGSIN présente le positionnement des différentes infrastructures technologiques supportant les fonctions et solutions technologiques.

Le concept de cloisonnement de l'AGSIN permet le découpage de zones de manière à gérer adéquatement les accès à celles-ci. Les équipements assurant le cloisonnement permettent une connexité sécuritaire entre les zones, entre les domaines de confiance et avec les clientèles en acceptant seulement les connexions autorisées. Les coupe-feu et/ou les routeurs sont généralement utilisés pour protéger les zones.

Les zones s'apparentent au concept de zone démilitarisée (DMZ). Par définition, une DMZ est une zone neutre entre l'Internet et le réseau interne. Cette zone ne se trouve pas sur le réseau interne mais n'est pas totalement ouverte sur l'Internet.

Le concept des zones de l'AGSIN propose un découpage facilitant la protection des informations numériques au niveau approprié (le découpage présenté est générique et adaptable à chaque domaine). Chaque zone contient un ensemble d'équipements informatiques de réseautique et de logiciels regroupés en fonction de certaines considérations qui sont précisées dans les pages qui suivent.

Les interfaces sécuritaires du modèle d'affaires utilisent les services fournis par les équipements et logiciels des zones et des cloisonnements afin d'offrir les fonctions de sécurité qu'elles requièrent.

Les réseaux de transport permettent l'échange des informations numériques et des informations de la base d'information en matière de sécurité. En portant une attention particulière aux réseaux de transport en terme de sécurisation, on permettra de ne pas affaiblir la sécurité des domaines de confiance.

Cloisonnement :

Les mécanismes de sécurité et les solutions technologiques assurant le cloisonnement comprennent principalement les coupe-feu, les routeurs, les routeurs avec fonction de coupe-feu et les commutateurs. Le choix des mécanismes de sécurité et des composantes ou solutions technologiques assurant le cloisonnement doit être fait en fonction de critères précis élaborés selon les besoins d'affaires et de sécurité des domaines de confiance.

Par définition, les coupe-feu sont des dispositifs informatiques qui permettent le passage sélectif des flux d'informations entre un réseau interne et un réseau public, ainsi que la neutralisation des tentatives d'intrusion en provenance du réseau public.

Essentiellement, les coupe-feu servent à délimiter des zones ayant différentes caractéristiques. Ils assurent le confinement sécuritaire des zones notamment en :

- n'acceptant que les accès autorisés (adresses et protocoles);
- cachant les adresses des serveurs (optionnel);
- bloquant systématiquement tous les autres accès. Si d'autres accès sont requis, ils doivent faire l'objet d'une évaluation selon les politiques et procédures du domaine de confiance.

Les routeurs acheminent des paquets de données sur un réseau de transport. Il ne faut pas confondre un routeur et une passerelle, même si les internautes ont eu tendance, à l'origine du moins, à employer passerelle (gateway) comme synonyme de routeur. Les routeurs permettent le transfert des paquets de données de manière sécuritaire notamment en :

- acceptant que les communications autorisées (adresses);
- cachant les adresses des serveurs (optionnel);
- refusant toutes les autres communications;
- offrant des fonctionnalités de coupe-feu via leur système d'opération (optionnel).

Les commutateurs permettent également l'acheminement des paquets de données sur un réseau de transport. Quoique plus limités que les routeurs, ils offrent la possibilité de filtrer les paquets de données au niveau des adresses. En ce sens, ils peuvent être utilisés dans certains cas pour le cloisonnement.

Il est généralement reconnu que les mécanismes de sécurité et les solutions technologiques assurant le cloisonnement ne sont pas suffisant pour assurer la sécurité des zones d'un domaine de confiance. Des mécanismes de sécurité et des solutions technologiques additionnels sont généralement requis dans les zones afin d'assurer une protection adéquate de l'information numérique.

Zone :

Les mécanismes de sécurité et les solutions technologiques additionnels requis pour la protection des zones d'un domaine de confiance sont ceux qui assurent principalement la fonction de surveillance. Des mécanismes de sécurité et des solutions technologiques assurant les autres fonctions peuvent également être utiles en fonction du niveau de protection et du contexte d'utilisation[108].

Deux zones spécifiques apparaissent dans la vue infrastructure technologique du modèle général de l'AGSIN afin de mettre en évidence leurs caractéristiques et de préciser les mesures de sécurité à mettre en place :

1. Zone d'administration et de surveillance :

Cette zone permet aux domaines de confiance d'administrer de façon sécuritaire et de surveiller en tout temps l'état des équipements informatiques (serveurs, équipements particuliers, etc.), des équipements de réseautique (aiguilleurs, coupe-feu, etc.) et des logiciels (systèmes d'exploitation, applications d'entreprises, SGBD, etc.) sous leur responsabilité.

La zone d'administration et de surveillance se situe derrière le cloisonnement le plus éloigné de la zone périmètre du domaine de confiance principalement en raison de la nature des informations et du type d'applications qu'elle contient. Les équipements et logiciels compris dans cette zone incluent notamment:

- Le(s) commutateur(s) et/ou le(s) concentrateur(s) servant à l'insertion d'équipements spécialisés dans la zone d'administration et de surveillance.
- La ou les console(s) d'administration et de surveillance nécessaires à la gestion d'un certain nombre d'informations de la base d'informations en matière de sécurité. Ces équipements et logiciels permettent d'administrer et de surveiller les divers mécanismes de sécurité et solutions technologiques (Information de paramétrisation, règles diverses en matière de sécurité, etc.). Considérant leur importance, ces équipements et logiciels doivent être hautement sécurisés.

2. Zone périmètre :

Cette zone permet aux domaines de confiance d'établir les différentes interconnexions nécessaires pour les échanges d'informations numériques avec d'autres domaines de confiance et avec les clientèles. Elle contient les équipements et logiciels nécessaires pour assurer une utilisation sécuritaire des réseaux de transports (RICIB et RETEM, Internet et autres).

La zone périmètre se situe devant le cloisonnement de premier plan du domaine de confiance. Les équipements et logiciels compris dans cette zone incluent notamment :

- Le(s) routeurs(s) qui établissent les interconnexions avec les autres domaines de confiance via les réseaux de transport (RICIB et RETEM, Internet et autres). Ces routeurs peuvent ou non appliquer des règles de filtrages en fonction des politiques d'interconnexion des domaines de confiance.
- Le(s) commutateur(s) et/ou le(s) concentrateurs servant à l'insertion d'équipements spécialisés dans la zone périmètre.

[108] On consultera la section 2.5 pour plus de détails sur les fonctions de sécurité, les mécanismes de sécurité et les solutions technologiques.

- Le(s) détecteurs d'intrusion réseau afin de surveiller les attaques et/ou les tentatives d'attaques au(x) aiguilleur(s) et/ou au(x) coupe-feu. Ce(s) détecteur(s) sont habituellement des agents[109] de surveillance installés sur des serveurs dédiés qui fondent leurs décisions sur des informations obtenues du réseau uniquement. Ces équipements et logiciels spécialisés sont branchés en permanence dans la zone périmètre. Considérant leur importance, ces équipements et logiciels doivent être hautement sécurisés.
- Le(s) analyseur(s) de vulnérabilités afin d'effectuer des vérifications sur la sécurité des équipements et logiciels accessibles de la zone périmètre. Le(s) analyseur(s) de vulnérabilités sont des équipements et logiciels spécialisés d'essais installés, au besoin, dans la zone périmètre. Les analyses de vulnérabilités effectuées dans cette zone permettront de s'assurer que les équipements et logiciels accessibles de cette zone tels le(s) aiguilleur(s) ou le(s) détecteurs d'intrusion réseau sont sécurisés et paramétrés adéquatement. Elles permettront également de s'assurer que les équipements de cloisonnement, tels les coupe-feu, les routeurs avec option de filtrage et les commutateurs intelligents sont sécurisés et paramétrisés adéquatement.

En ce qui concerne les zones 1 à n, chaque domaine de confiance doit déterminer le découpage des zones qui répondra adéquatement à ses besoins. Tel que mentionné précédemment, le concept de zone propose un découpage facilitant la protection des informations numériques au niveau approprié. La détermination des zones est principalement basée sur :

- le type d'équipements et de logiciels;
- le type d'information emmagasinée;
- le type de services offerts;
- le type d'accès autorisés.

À titre d'exemple, un domaine de confiance a déterminé qu'une zone particulière (appelée zone sensible pour les fins de l'exemple) est nécessaire pour protéger le serveur de base de données contenant des informations numériques sensible accessibles à partir du serveur Web de la zone accessible d'Internet (appelé zone publique pour les fins de l'exemple).

Une zone périmètre est donc nécessaire afin de protéger adéquatement les informations numériques sur le serveur de base de données et les échanges électroniques entre la zone sensible et la zone publique.

La zone sensible de notre exemple se situe derrière le cloisonnement de premier ou de deuxième plan du domaine de confiance et comprend des règles strictes d'accès entre les zone sensible et la zone publique.

Les équipements compris dans la zone publique incluent notamment :

- Le(s) commutateur(s) et/ou le(s) concentrateurs servant à l'insertion d'équipements spécialisés dans la zone périmètre.
- Le(s) détecteurs d'intrusions réseau afin de surveiller les attaques et/ou les tentatives d'attaques sur le segment de réseau de la zone sensible.
- Le(s) détecteurs d'intrusion serveur et SGBD afin de surveiller les attaques et/ou les tentatives d'attaques destinées au système d'exploitation et au SGBD. Ces détecteurs sont habituellement des

[109] Un agent est une entité logicielle qui effectue une certaine fonction de supervision sur une station hôte. Un agent peut réaliser une seule fonction très spécifique ou, au contraire, des activités beaucoup plus complexes.

agents de surveillance installés directement sur le(s) serveur(s) et fondent leurs décisions sur des informations obtenues de(s) serveur(s) uniquement.

- Le(s) analyseur(s) de vulnérabilités afin d'effectuer des vérifications sur la sécurité des équipements et logiciels accessibles de la zone sensible. Le(s) analyseur(s) de vulnérabilités sont des équipements et logiciels spécialisés d'essais installés au besoin dans la zone sensible. Les analyses de vulnérabilités effectués dans cette zone permettront de s'assurer que les équipements accessibles de cette zone tels le(s) aiguilleur(s), le(s) détecteurs d'intrusion réseau sont sécurisés et paramétrisés adéquatement. Elles permettront également de s'assurer que les équipements de cloisonnement, tels les coupe-feu, les aiguilleurs avec option de filtrage, les commutateurs intelligents sont sécurisés et paramétrisés adéquatement.
- Le serveur de base de données contenant les informations sensibles. Les fonctions de sécurité pour assurer une haute disponibilité du serveur de base de données, pour assurer un contrôle d'accès approprié au SGBD, etc., sont autant d'éléments qui viendront protéger adéquatement les informations numériques emmagasinées sur le serveur de base de données et les échanges électroniques entre la zone sensible et la zone publique.

Réseau gouvernemental (le RICIB et le RETEM) :

Quoique la section 4 traite plus spécifiquement du RICIB et du RETEM, la vue infrastructure technologique du modèle général de l'AGSIN attire l'attention sur le réseau gouvernemental afin de faire ressortir les aspects en matière de sécurité propres à cette infrastructure commune.

Le RICIB et le RETEM, en tant qu'infrastructure commune, se doivent d'assurer la protection des informations numériques échangées sur ce réseau. Ils offrent donc un potentiel intéressant de mise en commun des mécanismes de sécurité et des solutions technologiques supportant les fonctions de sécurité relatives aux réseaux.

Cette mise en commun permettra non seulement d'uniformiser l'administration et la surveillance du RICIB et du RETEM mais permettra également de faciliter et d'accélérer le processus de raccordement et de support aux domaines de confiance sous la gouvernance de l'État nécessitant les services du RICIB et du RETEM.

La définition d'ententes de raccordement et d'utilisation ainsi que d'interfaces sécuritaires communes pourraient grandement contribuer à cet effet de levier.

3.4.2 Potentiel de mise en commun, de partage ou de réutilisation

Les infrastructures technologiques nécessaires aux solutions technologiques supportant les mécanismes de sécurité qui assurent les fonctions de sécurité peuvent être dédiées au DC ou être de nature commune, partagée ou réutilisable.

Plusieurs infrastructures technologiques en matière de sécurité de l'information numérique ont un potentiel intéressant de mise en commun[110], de partage ou de réutilisation. Cette section décrit ces infrastructures technologiques ainsi que le contexte d'utilisation.

[110] L'ICPG, le répertoire gouvernemental et GIRES sont déjà retenus comme infratructures communes par le SCT. Cependant, il reste des travaux afin de savoir qui, quoi, quand, comment, etc. sera mis en commun.

Potentiel de mise en commun :

- Infrastructures technologiques en matière de sécurité :
  - Plusieurs solutions technologiques (équipements et logiciels) supportant les mécanismes de sécurité pourraient éventuellement être mis en commun afin d'uniformiser les façons de faire au sein de l'appareil gouvernemental. Ces solutions technologiques comprennent :
    - Le(s) serveur(s) du répertoire gouvernemental des employées;
    - Le(s) serveur(s) du répertoire gouvernemental des mandataires/partenaires;
    - Le(s) serveur(s) de gestion des clés et des certificats des employé(e)s;
    - Le(s) serveur(s) de gestion des clés et des certificats des mandataires/partenaires;
    - Le(s) serveur(s) de gestion des clés et des certificats du pivot;
    - Le(s) serveur(s) de détecteurs d'intrusions réseau et de virus du RICIB et du RETEM;
    - Le(s) analyseur(s) de vulnérabilités réseau du RICIB et du RETEM;
    - Le(s) serveur(s) coupe-feu du RICIB et du RETEM;
    - Le(s) aiguilleur(s) du RICIB et du RETEM;
    - Le(s) serveur(s) RPV du RICIB et du RETEM.
    - Le(s) serveurs(s) de détecteurs des virus;
    - Le(s) serveurs(s) coupe-feu de l'intranet gouvernemental;
    - Le(s) serveurs(s) de contrôle d'accès (unifiés);
    - Le(s) détecteur(s) d'intrusions serveur;
    - Le(s) analyseur(s) de vulnérabilités serveur;
    - Le(s) moniteur(s) de contenu actif.
  - D'autres équipements, logiciels et serveurs en matière de sécurité pourraient être mis en commun dépendamment des orientations gouvernementales.

Potentiel de partage :

- Serveur(s) du registre-référentiel des schémas XML de sécurité normalisés à la DGT;
  - Les modèles d'interopérabilité basés sur XML sont très flexibles en ce qui a trait aux degrés possibles de partage réutilisation des métadonnées.
- Infrastructures technologiques en matière de sécurité des secteurs de la santé, de l'Éducation et municipal :
  - Plusieurs solutions technologiques de ces secteurs supportant les mécanismes de sécurité pourraient éventuellement être partagés afin d'uniformiser les façons de faire au sein de ces secteurs. Ces composantes ou solutions technologiques comprennent :
    - Le(s) serveur(s) de détecteurs des intrusions réseau et de virus des réseaux sectoriels;
    - Le(s) analyseur(s) de vulnérabilités des réseaux sectoriels;
    - Le(s) serveur (coupe-feu des réseaux sectoriels);
    - Le(s) aiguilleur(s) des réseaux sectoriels;
    - Le(s) serveur(s) RPV des réseaux sectoriels.

  - D'autres équipements, logiciels et serveurs en matière de sécurité de ces secteurs pourraient être partagés dépendamment de ces derniers.
- Infrastructures technologiques en matière de sécurité propres à une grappe.

Potentiel de réutilisation :

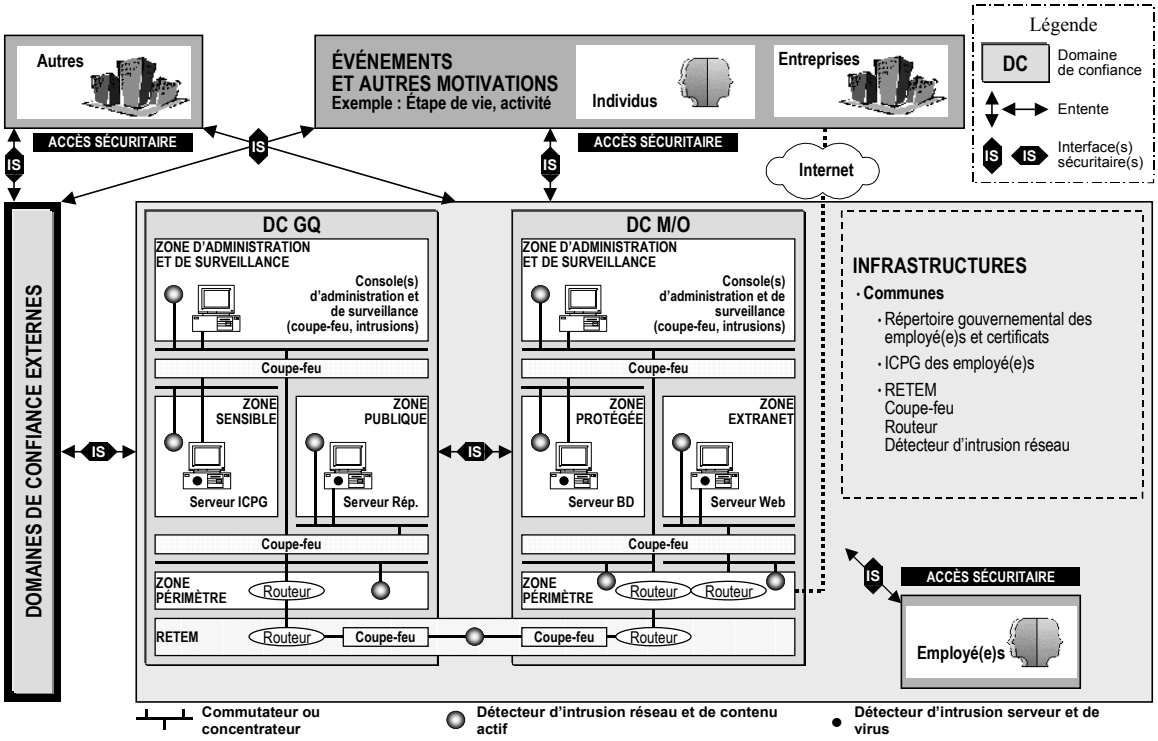
- Aucun potentiel identifié.

3.4.3 Exemple

Pour compléter l'exemple de l'Extranet d'un M/O offrant aux entreprises abonnées la possibilité de transmettre un formulaire électronique, il est impératif de protéger les informations, applications et équipements par des infrastructures technologiques supportant le processus d'affaires électroniques.

La figure suivante illustre le découpage technologique de chaque domaine de confiance requis pour assurer la protection du processus d'affaires électroniques.

PRINCIPALES INFRASTRUCTURES TECHNOLOGIQUES



Sans être exhaustif, le découpage technologique présente les principaux mécanismes de sécurité et solutions technologiques nécessaires afin de créer les zones requises et d'assurer le cloisonnement nécessaire à la sécurité du processus d'affaires électroniques.

Outre la zone périmètre et la zone d'administration et de surveillance explicitée à la section précédente, chaque zone identifié des domaines de confiance inclut notamment :

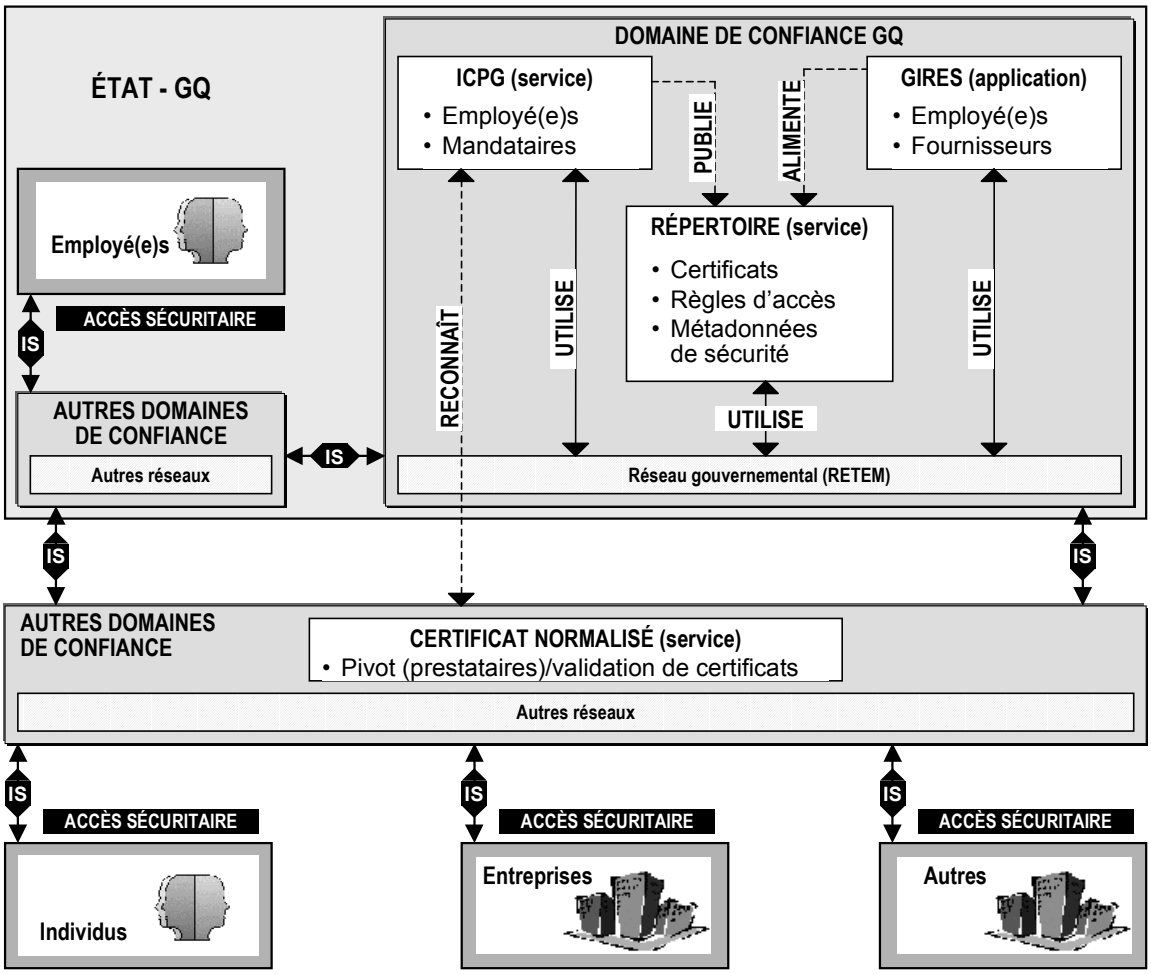
- Un commutateur et/ou un concentrateur servant à l'insertion d'équipements spécialisés dans la zone (ex. : analyseurs de vulnérabilités au besoin).
- Des détecteurs d'intrusions réseau et de contenu actif afin de surveiller les attaques et/ou les tentatives d'attaques sur le segment de réseau de la zone.
- Des détecteurs d'intrusions serveur et de virus afin de surveiller les attaques et/ou les tentatives d'attaques destinées au système d'exploitation ainsi qu'aux applications s'exécutant sur le serveur et/ou au SGBD. Ces détecteurs sont habituellement des agents de surveillance installés directement sur le(s) serveur(s) et fondent leurs décisions sur des informations obtenues de(s) serveur(s) uniquement.
- Les serveurs d'applications spécifiques équipés des fonctions de sécurité nécessaires pour assurer notamment le niveau de disponibilité requis, le contrôle d'accès approprié, etc. sont autant d'éléments qui viendront protéger adéquatement les serveurs spécifiques à chaque zone.

4. POSITIONNEMENT DES PROJETS SPÉCIFIQUES

Cette section présente le positionnement de l'ICPG, du répertoire gouvernemental, de GIRES et du réseau gouvernemental RETEM par rapport à l'architecture gouvernementale de la sécurité de l'information numérique.

La figure suivante illustre la vision gouvernementale cible des relations anticipées entre ces services communs et applications communes.

VISION GOUVERNEMENTALE CIBLE
Relations ICPG – Répertoire – GIRES – RETEM
Aspect sécurité



Quoique tous les aspects de ces services communs et applications communes n'aient pas encore été couverts et que certains travaux soient actuellement en cours ou sur le point de démarrer à cette fin, cette vision permet de présenter à haut niveau, l'aspect sécurité relié à ces services et applications. Actuellement, l'utilisation prévue en matière de sécurité des services communs et applications communes se définit de la manière suivante :

ICPG et certificat normalisé

- L'ICPG vise à offrir des services de gestion des clés et des certificats aux clientèles employé(e)s et mandataires. L'ICPG utilisera le répertoire gouvernemental afin de publier, notamment, les clés et les certificats des clientèles desservies.

- Le certificat normalisé vise à définir une norme sur l'émission de clés et de certificats pour sécuriser les transactions électroniques au sein du gouvernement, ainsi qu'entre le gouvernement et les clientèles externes. Grâce au pivot (autorité de liens), il sera possible de reconnaître les clés et les certificats des clientèles individus, entreprises ou autres utilisatrices des services des prestataires de gestion des clés et des certificats accrédités par le gouvernement. Bien que la figure précédente puisse laisser croire que le pivot sera à l'extérieur du gouvernement, sa localisation (interne, externe ou en partenariat) reste à déterminer.

GIRES

- GIRES vise à offrir un ensemble d'applications en ressources humaines, financières et matérielles. GIRES possédera l'information la plus à jour sur les employé(e)s et les fournisseurs pour alimenter le répertoire gouvernemental.

Répertoire gouvernemental

- Le répertoire gouvernemental sera associé à trois fonctions principales soit localiser, garantir et partager. Le répertoire gouvernemental sera un élément fondamental de la sécurité. Il offrira la capacité d'héberger notamment des clés et des certificats, des règles d'accès et des métadonnées de sécurité.

RETEM

- Le RETEM vise à offrir des services d'échanges électroniques sécuritaires au sein de l'appareil gouvernemental. Le RETEM sera donc utilisé par l'ICPG, le répertoire gouvernemental et le certificat normalisé ainsi que par l'application GIRES pour toutes les communications entre ces derniers avec un niveau de sécurité approprié.

Les sous-sections suivantes décrivent en détails le positionnement de l'ICPG, du répertoire gouvernemental, de GIRES et du réseau gouvernemental RETEM.

4.1 ICPG

La mise en place de l'ICPG implique des enjeux socio-économiques, organisationnels, technologiques et juridiques dont toutes les composantes et conséquences ne sont pas encore totalement définies. Toutefois, pour assurer la cohérence et l'optimisation des ressources dans l'implantation de l'ICPG, des orientations

fondamentales ont été adoptées par le Conseil du Trésor le 29 juin 1999. Sur la base d'un examen de la structure des ICP gouvernementales existantes ou proposées aux plans national et international, un modèle fonctionnel adapté au fonctionnement gouvernemental a été choisi.

4.1.1 Positionnement de l'ICPG

L'élaboration de l'infrastructure à clés publiques gouvernementale s'inscrit à l'intérieur de la Politique québécoise de l'autoroute de l'information.

L'infrastructure à clés publiques gouvernementale, dont l'institution a été autorisée par le Conseil du Trésor le 29 juin 1999, concerne un ensemble d'acteurs, de pratiques et de technologies dédiés à la gestion de clés et de certificats de chiffrement (passeports et visas électroniques) permettant à des personnes de se reconnaître à distance, d'effectuer en toute sécurité des transactions électroniques et d'échanger de l'information numérique de nature délicate.

L'ICPG vise donc à répondre à ces besoins en garantissant, par l'usage de différents types de certificats et de la cryptographie, l'intégrité et la confidentialité de l'information numérique, l'authentification des utilisateurs et l'irrévocabilité des documents qu'ils rédigent et des actions qu'ils posent. Son implantation est en cours conformément au modèle fonctionnel approuvé par le Conseil du trésor.

L'objectif est de faire en sorte que, progressivement, d'ici 2004, les employés de l'État dont les fonctions impliquent une interaction avec des données confidentielles ou la nécessité d'authentifier leur identité ou celle de leurs interlocuteurs, disposent d'un passeport et des visas électroniques nécessaires pour transiger avec des clientèles disposant de passeports et de visas électroniques équivalents.

En juillet 2000, un rapport intitulé Modèle fonctionnel d'une infrastructure à clés publiques gouvernementale est présenté au SCT. Le but de ces travaux est de définir un modèle interopérable qui permet la cohabitation de solutions provenant de différentes autorités de certification et de différents fournisseurs. Ce document vise à compléter celui intitulé : Document de travail sur la gestion de clés et de certificats au gouvernement du Québec dans sa version 3.0 du 31 mars 1999, issu du SCT dont la version 4 va devenir une directive.

Ce document se situe en amont d'une politique de certification (future directive) et décrit l'ensemble des éléments à prendre en compte lors de la conception de l'ICPG. La première partie du document décrit les fonctionnalités d'une ICP. La deuxième partie soulève les notions importantes quant à la gestion des certificats. De par son importance, la problématique des chemins de certification est abordée dans la troisième partie. Ensuite, un modèle opérationnel de l'ICPG favorisant l'interopérabilité est proposé.

De plus, en mars 2000, une étude intitulée « Bilan des projets et impact des infrastructures à clés publiques », dans le cadre du positionnement du gouvernement du Québec par rapport aux infrastructures à clés publiques a été produit. Ce document a pour objectif de tracer un bilan réaliste des projets des ministères et organismes, en cours ou à venir, avec un potentiel d'utilisation de l'ICP ou de tout autre moyen de sécurisation des accès électroniques des employés et des clientèles du gouvernement. Ce rapport présente les résultats de l'analyse et un certain nombre de recommandations afin d'éclairer le SCT relativement à un positionnent gouvernemental face à l'ICP, à l'établissement d'une ICPG et à la mise en place du concept de « Certificat Québec ».

Dans le cadre du projet « Certificat Québec », le SCT a mis sur pied un groupe de travail pour la définition de la ou des normes sur la délivrance et la gestion des clés et des certificats pour sécuriser les transactions électroniques au sein du gouvernement, ainsi qu'entre le gouvernement et les individus/entreprises du

Québec. Ce groupe de travail a pour mandat global de remettre au Conseil du trésor un rapport de conception du certificat normalisé afin d'appuyer le démarrage des travaux du comité de normalisation qui sera piloté par le Bureau de Normalisation du Québec.

Il est également à noter qu'afin de faciliter la mise en oeuvre de l'ICPG, le SCT sélectionnera sous peu un ou plusieurs produits d'ICP. Le ou les produits d'ICP retenus serviront à émettre et à gérer les certificats des clientèles gouvernementales.

4.1.2 Les clientèles visées

La délivrance des clés et certificats à l'ensemble des acteurs impliqués dans les échanges et les transactions électroniques gouvernementales soulève non seulement des questions d'organisation interne, mais aussi et surtout des questions d'adhésion des utilisateurs.

On distingue quatre (4) types de clients certifiés par le gouvernement dans le cadre de l'ICPG (directement ou via des ententes qui s'appuient sur le certificat normalisé), chacun présentant des caractéristiques particulières, à savoir:

- Les employés de l'état, qui sont des usagers aux caractéristiques homogènes et pour lesquels la mise en place des mesures de sécurité est entièrement sous le contrôle du gouvernement du Québec;
- Les mandataires du gouvernement du Québec et de ses clients qui, à des degrés divers, sont intégrés aux processus d'affaires des ministères et organismes concernés. Ceux-ci font le lien entre l'individu ou l'entreprise et le gouvernement du Québec;
- Les associations et les entreprises, que ce soit pour s'acquitter de leurs obligations légales ou fiscales ou pour offrir des biens et services dans le cadre des marchés publics. Les fournisseurs sont également une clientèle faisant des échanges avec le gouvernement;
- Les individus, lesquels sont directement concernés par les problématiques de respect de la vie privée et de protection des renseignements personnels.

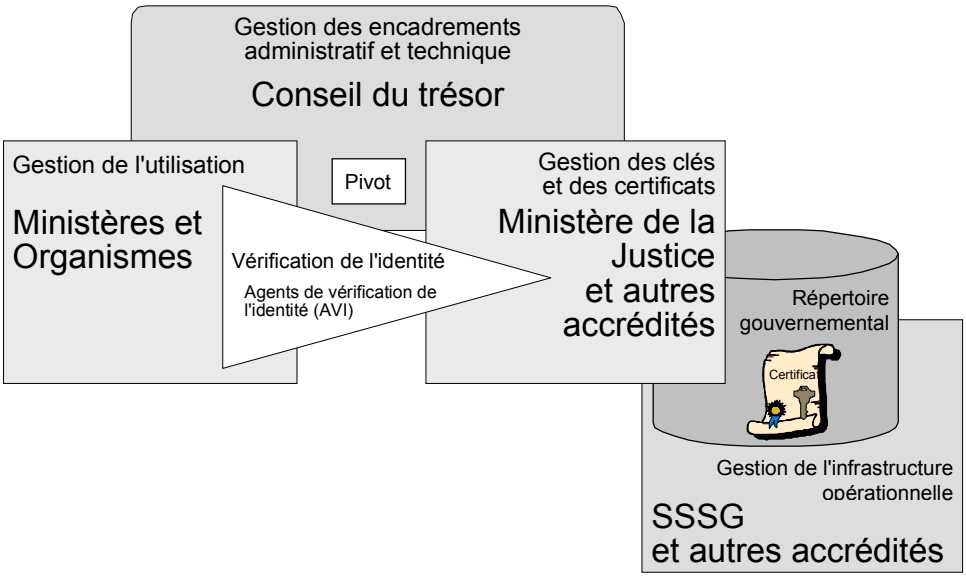
Les problématiques reliées à chacun des types d'utilisateurs diffèrent les unes des autres et le SCT est à développer des approches adaptées à ces conditions particulières.

4.1.3 Le modèle fonctionnel

Le modèle fonctionnel de l'ICPG est celui adopté par le Conseil du trésor du Québec dans sa décision du 29 juin 1999. Ce modèle est illustré ci-après. Il comporte les fonctions suivantes: la gestion des encadrements administratif et technique, la gestion de l'utilisation, la vérification de l'identité, la gestion des clés et des certificats, la gestion de l'infrastructure technologique.

La description des principales fonctionnalités du modèle fonctionnel de l'ICPG se présente comme suit:

MODÈLE FONCTIONNEL DE L'ICPG



Gestionnaire des encadrements administratif et technique (GEAT)

Cette fonction consiste à assurer, par des politiques, directives, normes et guides de fonctionnement, la cohérence requise pour permettre le fonctionnement efficace de l'ICP ainsi que la reconnaissance réciproque et l'interconnexion avec d'autres services de certifications externes autorisés par des ententes à cet effet.

Le GEAT est aussi chargé, sous réserve des exigences de la loi en matière d'ententes internationales et intergouvernementales, de convenir d'accords de reconnaissance réciproque avec des autorités de certification externes qu'il juge opportun de conclure. Le GEAT agit comme prestataire de services de certification vis-à-vis des parties externes au gouvernement.

Plus précisément , le GEAT:

- Assure, par le biais de directives, de guides de fonctionnement et de normes techniques afférentes, la coordination des diverses composantes de l'ICPG et l'interopérabilité de leur fonctionnement;
- Conclut, sous réserve des exigences de la loi en matière d'ententes internationales et intergouvernementales, les ententes de reconnaissance réciproque avec d'autres infrastructures à clés publiques et l'interconnexion avec d'autres services de certification qu'il juge opportunes et qui s'imposent alors à l'ensemble de l'ICPG;
- Désigne les gestionnaires des clés et des certificats, les gestionnaires de l'infrastructure opérationnelle et les AVI;
- Accrédite les applications autorisées;
- Détermine les cas où l'utilisation de l'ICPG est obligatoire;
- Élabore le concept de pivot (autorité de liens) et voit à sa mise en oeuvre.

Le pivot

Le pivot est une autorité de liens qui contrôle et gère tous les services de certifications intra et intergouvernementaux et les liens entre le gouvernement et le privé. La gestion de cette autorité est assurée par le Conseil du trésor dans l'exercice de ses fonctions de GEAT. Son rôle est de permettre aux différentes infrastructures en place ou futures d'être interconnectées et d'échanger en toute confiance tout en gérant leur propre politique de confiance. L'autorité de liens n'est pas une autorité de certification racine, elle permet seulement de connecter les différentes infrastructures, soit différents domaines de confiance entre eux en partageant un même niveau de confiance.

Gestionnaire de l'utilisation (GU)

Cette fonction consiste à autoriser l'attribution (délivrance et révocation) des certificats électroniques aux abonnés de l'ICPG. Elle détermine les niveaux de confiance requis pour chacun des processus d'affaires concernés, les personnes qui auront accès à des clés ainsi que leurs obligations et privilèges relativement à l'ICP. Le GU a également la responsabilité d'adopter les usages et les pratiques d'utilisation des certificats et de vérifier leur mise en application concrète. Les ministères et organismes sont les responsables de la gestion de l'utilisation de l'ICPG.

Gestionnaire des clés et des certificats (GCC)

Cette fonction consiste à délivrer, révoquer et suspendre les clés et les certificats des abonnés (sauf des agents de vérification de l'identité et des GCC) et à réaliser les activités opérationnelles du processus de certification dont, notamment, signer les certificats, publier dans l'annuaire X.500/LDAP relativement aux certificats et produire des listes de certificats en vigueur ou révoqués. Il assure aussi la mise en application des ententes de reconnaissance réciproque conclues par le GEAT avec des AC externes.

Le gestionnaire des clés et des certificats (GCC) est responsable de l'ensemble des composantes matérielles, logicielles, humaines et organisationnelles associées au cycle de vie des clés et des certificats. Cette fonction consiste par exemple à:

- Recevoir et coordonner les demandes de certificats
- Ouvrir et mettre à jour des dossiers d'abonnés
- Générer, délivrer et publier des certificats de signature numérique
- Gérer le répertoire où sont conservés les certificats
- Garantir l'intégrité des certificats tout au long de leur cycle de vie
- Diffuser l'information sur les certificats révoqués
- Appliquer les ententes de reconnaissance réciproque avec d'autres autorités de certification
- Etc.

Gestionnaire de l'infrastructure opérationnelle (GIO)

Cette fonction consiste, sur désignation du GEAT, à assurer les activités techniques et opérationnelles déléguées par le GCC et supportant celui-ci, à voir à la sécurité des appareils et des logiciels utilisés par le gestionnaire des clés et des certificats et à assurer le service technique à la clientèle. Le responsable de

cette fonction développe, installe, opère et entretient les infrastructures matérielles et logicielles nécessaires pour supporter le GCC.

Agent de Vérification de l'identité (AVI)

Cette fonction consiste à exécuter les tâches de vérification individuelle de l'identité des personnes et les activités connexes. Elle peut également consister à contrôler un dispositif, une application ou un processus (p. ex. un site Web). La fonction de l'agent de vérification de l'identité est au cœur du réseau de confiance que vise à établir l'ICP puisqu'elle assure le lien de confiance nécessaire entre une paire de clés et une personne, un dispositif, une application ou un processus. La qualité de la vérification de l'identité est essentiellement liée à la compétence de la personne qui l'exerce. L'AVI doit constater personnellement ce qu'il a pour fonction de vérifier et le certifier lui-même pour assurer l'authenticité de l'opération.

4.1.4 Désignations

Dans l'exercice de ses fonctions de Gestionnaire des encadrements administratif et technique, le Conseil du trésor a désigné, le 27 février 2001, la Direction générale des services de justice du ministère de la Justice (DGSJ) comme gestionnaire de clés et certificats pour répondre aux besoins de certification des employés, dispositifs et applications de l'État et des mandataires du gouvernement ou de ses clients, à condition que la vérification d'identité soit faite, lors d'une entrevue, par un Agent de vérification de l'identité (AVI) autorisé par le Secrétariat du Conseil du trésor. D'ici le 7 octobre 2003, le MJQ agira également comme gestionnaire des infrastructures opérationnelles permettant de répondre à ces besoins de certification des ministères et organismes. À partir du 7 octobre 2003, le SSSG prendra la relève de la partie assumée par la firme LGS pour le MJQ comme gestionnaire des infrastructures opérationnelles.

Le SSSG interviendra d'ici le 7 octobre 2003 sur les besoins de certification s'adressant à des employés, applications et dispositifs de l'État, dans les cas où:

- le MJQ n'est pas en mesure de délivrer des clés et certificats dans un contexte particulier ;
- l'identification des usagers est établie par le M/O.

Le SSSG agira également pendant cette période comme gestionnaire des infrastructures opérationnelles permettant de répondre à ces besoins de certification des M/O.

4.1.5 La sécurité particulière à l'ICPG

L'ICPG vise à répondre aux besoins de permettre à des personnes, applications et dispositifs de se reconnaître à distance, d'effectuer en toute sécurité des transactions électroniques et d'échanger de l'information numérique de nature délicate.

Dans cette mesure, il se doit lui-même d'être protégé afin d'offrir un niveau adéquat de disponibilité, d'intégrité et de confidentialité des informations numériques emmagasinées, traitées et échangées lors des communications avec le serveur de clés et de certificats. De plus, l'authentification des utilisateurs habilités au niveau approprié et, le cas échéant, l'irrévocabilité des communications entre l'utilisateur et le serveur de clés et de certificats devront être garanties.

Au niveau juridique, la loi concernant le cadre juridique des technologies de l'information en ce qui a trait à l'utilisation du répertoire pour rendre public les certificats de chiffrement amènera des obligations qui se traduiront en besoins de sécurité organisationnels et technologiques. À cet effet, la loi contient des dispositions pour baliser la prestation de services de certification et de répertoire et offre à tout prestataire de services de certification, qu'il soit du Québec ou d'ailleurs, de se faire accréditer, en fonction des mêmes critères d'appréciation, par une personne ou un organisme déterminé par le gouvernement. De plus, dépendant de la nature des informations numériques emmagasinées, traitées et échangées sur le serveur de clés et de certificats, d'autres lois pourraient préciser des éléments additionnels à considérer.

Du côté organisationnel et humain, l'infrastructure à clés publiques nécessite une répartition adéquate des responsabilités entre les organismes exerçant des fonctions centrales, communes ou partagées. À cet effet, le modèle fonctionnel de l'ICPG établit le découpage requis. Il est donc primordial que les besoins en terme de sécurité administrative et organisationnelle ainsi que du personnel responsable de l'ICPG soient adressés de manière précise et se reflètent par l'adoption d'une politique de certificats (par le GEAT) et l'établissement de pratiques et procédures de certification par les gestionnaires de clés et certificats désignés par le Conseil du trésor. De plus, des considérations importantes au niveau de la sécurité physique et du milieu de l'ICPG amèneront à intégrer dans la politique de certification des mesures spécifiques dans ce domaine. Les besoins au niveau de la sécurité opérationnelle sont également importants et devront se traduire notamment au niveau des procédures et des guides d'opération ainsi qu'au niveau des mesures de surveillance, de détection et d'urgences.

Du côté technologique, plusieurs considérations permettent d'établir qu'il existe des besoins importants en matière de sécurité au niveau du matériel, des logiciels et des communications. Ces besoins se traduisent principalement au niveau de la normalisation de la configuration et de l'administration sécuritaire de l'ICPG ainsi que sur la mise en place et la gestion d'outils de prévention, de détection et de correction. De plus, des considérations importantes au niveau des acquisitions et du développement de systèmes (ex. : règles de développement d'interfaces) permettront de contribuer à l'interopérabilité de l'ICPG avec d'autres ICP de différents paliers gouvernementaux et du secteur privé. Une ICP doit être conçue et opérée de façon sécuritaire pour conserver un niveau de confiance donné.

4.1.6 L'arrimage avec les infrastructures gouvernementales

4.1.6.1 L'arrimage avec GIRES

Telle que définie dans la solution GIRES, l'utilisation de l'ICPG est associée aux pages blanches du répertoire gouvernemental en ce qui concerne les employés de l'état. L'ICPG pourrait permettre, par la gestion des clés publiques et l'émission des certificats, d'assurer :

- L'identification/authentification ;
- L'habilitation/contrôle d'accès ;
- La confidentialité ;
- L'intégrité ;
- L'irrévocabilité.

Les orientations de la solution GIRES précisent que, à prime abord, GIRES n'a pas besoin d'une ICP. Selon le sous-secrétariat à la gestion des ressources, la solution pourrait très bien fonctionner à l'aide de l'authentification disponible avec Oracle, à savoir un code d'utilisateur et un mot de passe avec

chiffrement de l'information lors des communications. Toutefois, les orientations gouvernementales en matière de sécurité de l'information et des échanges électroniques font en sorte qu'il est probable qu'une ICP sera nécessaire à la solution GIRES dès lors que les documents ne seront plus signés sur papier mais en mode électronique.

Pour l'instant, l'orientation retenue préconise l'utilisation des fonctions de base de sécurité fournies avec Oracle et la réalisation d'analyses plus poussées afin d'établir si l'utilisation de certificats de clés publiques, de chiffrement ou autres seront nécessaires pour certaines des transactions de la solution GIRES. La firme Oracle doit fournir à la solution GIRES toutes les fonctionnalités relatives à l'ICP avec la version 11i.3 .

4.1.6.2 L'arrimage avec le répertoire gouvernemental

Dans le rapport de conception détaillée du répertoire gouvernemental, il est mentionné que ce dernier est basé sur la norme X.500 et LDAP et vise à offrir les services de :

- Pages blanches qui fournissent l'information permettant de rejoindre une personne, plus précisément un employé du gouvernement;
- Pages bleues qui servent à repérer et rejoindre une organisation;
- Pages vertes qui fournissent l'information permettant de repérer un document et d'y avoir accès;
- Pages jaunes qui contiennent les données sur les fournisseurs.

Dans le cadre de l'AGSIN, il y a nécessité d'utilisation du répertoire gouvernemental pour les certificats de clés publiques des employés de l'état et des mandataires. Il y a un lien étroit entre le répertoire gouvernemental et l'ICPG, dont :

- Les services de répertoire des certificats de clés publiques de l'ICPG pour les employés de l'état et les mandataires en réponse aux utilisateurs et aux applications;
- La liste des certificats révoqués (CRL) pour les employés de l'état et les mandataires dépendant de la politique de confiance et de son pendant de politique de certification qui sera adoptée.

Mentionnons que selon les orientations du Conseil du trésor, il n'y aura pas d'autorité de certification dans chaque M/O.

D'autre part, en liaison avec les travaux du certificat normalisé, il est envisagé la mise en place d'un pivot qui aurait notamment pour fonction de constituer et tenir à jour un répertoire des prestataires de services de certification répondant à la norme. Seules les données nécessaires au bon fonctionnement de l'ICPG et pour la validation du certificat normalisé seraient publiés dans ce répertoire.

Ces données sont :

- La liste des certificats croisés des autorités de certification avec le pivot;
- La liste des certificats révoqués d'autorités de certification croisés des GCC de l'ICPG et des autres autorités dans l'ICPG.

Par ailleurs, pour fins de validation des certificats de signature des abonnés, le SCT envisage d'utiliser le protocole OCSP, évitant ainsi la consultation massive des listes de certificats révoqués de chaque Gestionnaire de clés et certificats.

4.1.7 Concordance de l'ICPG avec l'AGSIN

L'architecture gouvernementale de la sécurité de l'information numérique propose un ensemble de fonctions et de mécanismes afin d'assurer la sécurité de l'information numérique et les échanges électroniques appuyé par le concept de domaines de confiance. L'ICPG couvre les fonctions suivantes:

- L'identification/authentification ;
- L'habilitation/contrôle d'accès ;
- La confidentialité ;
- L'intégrité ;
- L'irrévocabilité.

L'usage de l'ICPG sera conséquent au résultat des travaux relatifs à la catégorisation de l'information numérique de manière à sécuriser cette information en fonction de la valeur établie. Principalement, l'ICPG répond à plusieurs des fonctions de sécurité et implique l'utilisation des mécanismes correspondants.

En terme d'arrimage avec l'AGSIN, il faudra tenir compte des travaux inhérents aux certificats normalisés. Le SCT a réalisé une étude concernant l'adhésion des intervenants publics et privés relativement à l'implantation d'un certificat normalisé pour l'ensemble du Québec, répondant aux meilleures pratiques de délivrance et de gestion reconnues au plan international.

Une opération formelle de normalisation du contenu et des processus de délivrance et de gestion des clés et certificats numériques sera entreprise. L'objectif est de permettre à la clientèle des services privés de certification d'utiliser leur certificat pour transiger avec le gouvernement. Le certificat normalisé se veut être un certificat à clés publiques reconnu par une large communauté d'utilisateurs et offrant une confiance suffisante dans l'identité du détenteur de la clé publique à la sécurisation de la plupart des échanges électroniques pouvant transiger sur le tronçon québécois de l'inforoute. Ce certificat serait émis et géré de la même manière par des autorités de certification reconnues et serait donc normalisé.

Un utilisateur potentiel de la clé publique pourrait s'attendre à un format de certificat identique et à une gestion de son cycle de vie identique, et donc à un niveau de confiance invariable. En conséquence, l'interopérabilité du certificat d'un champ d'application à l'autre en serait simplifiée, et deviendrait donc plus facilement réalisable.

Enfin, l'arrimage devra se faire avec l'AGSIN au niveau de l'usage de certaines normes. En effet, il y a deux types de requêtes de certificats, la requête faite à l'autorité de certification et celle faite au répertoire des clés publiques.

- Le premier type de requête est basé notamment sur la norme PKIX de l'IETF et aussi sur le standard de facto PKCS #10. La norme PKIX étant récente, elle n'est pas encore très répandue dans les logiciels commerciaux, mais l'engouement pour les réponses qu'elle apporte aux lacunes d'interopérabilité fait en sorte qu'elle pourrait être la norme la plus utilisée dans un futur très proche. La norme PKC#10 est plus répandue, mais elle ne couvre pas toutes les fonctionnalités nécessaires au bon fonctionnement d'une ICP;

- Le deuxième type de requête, celle au répertoire de clés publiques afin de localiser une clé d'un destinataire ou d'avoir accès à la liste des certificats révoqués, est principalement basée sur le protocole LDAP selon divers critères de recherche (ex : adresse de courriel ou nom). L'utilisation de On line Certificate Status Protocol (OCSP) issu du standard RFC-2560 de l'IETF qui permet de valider l'état (valide, révoqué ou suspendu) en ligne d'un certificat de façon rapide devra être précisée dans l'ICPG.

4.1.8 Conclusion

Il est important en rapport avec l'ICPG de considérer les éléments suivants :

- L'ICP n'est pas qu'un moyen de sécurité. Il s'agit également d'un moyen d'assurer l'apposition d'une signature juridiquement reconnue à un document qui pourra par la suite servir de preuve d'une transaction électronique;
- Lorsque applicable (c'est-à-dire selon la valeur de l'information numérique à protéger), l'ICPG est la seule solution de sécurité retenue par le SCT garantissant l'authentification forte et l'irrévocabilité ;
- L'infrastructure à clés publiques gouvernementale doit faire l'objet d'une gestion saine, coordonnée et soutenue de la part de tous les intervenants qui en sont responsables. C'est pourquoi le Conseil du trésor assume la fonction de gestionnaire des encadrements administratif et technique. La robustesse (aux niveaux organisationnel, humain, technologique et juridique) de l'ensemble et le niveau de confiance que cette robustesse lui permet d'offrir sont d'une extrême importance pour la reconnaissance juridique des transactions électroniques qu'elle supporte. Par exemple, la gestion des infrastructures technologiques doit couvrir toutes les facettes du cycle de vie des systèmes informatiques, y compris la spécification, l'installation, la configuration, les opérations, ainsi que le soutien et l'évolution technologique et opérationnelle. Par ailleurs, l'utilisation de l'ICPG dans les applications requiert que l'analyse des enjeux légaux (ex. prise en compte de la loi sur le cadre juridique des TI) soit complétée et que des solutions communes soient développées si l'on souhaite garantir une implantation efficace de la solution et ainsi permettre la reconnaissance éventuelle de ses transactions numériques devant les tribunaux. Les travaux de développement d'un guide en gestion intégrée des documents abordent directement ces questions;
- La mise en œuvre d'une infrastructure à clés publiques est un projet de grande envergure pour une organisation;
- Dans les divers projets en cours ou réalisés au sein des M/O, le gouvernement du Québec a utilisé divers logiciels d'ICP. Le choix gouvernemental définitif n'est pas encore arrêté. Diverses considérations de fonctionnalité, de sécurité et de coût doivent être examinées avant qu'une décision soit prise ou qu'une entente globale puisse être conclue avec un ou plusieurs fournisseurs de logiciels pour couvrir l'ensemble des clés et des certificats nécessaires à l'ICPG;
- La réutilisation, au bénéfice de l'ensemble des M/O des investissements faits par le gouvernement pour développer de nouvelles façons de faire qui intègrent l'ICPG a été favorisée. Ainsi l'ICPG présente un exemple évident de mise en commun notamment pour les employés de l'état et les mandataires;
- Des travaux subséquents restent à compléter, soit principalement au niveau de :
  - la gouvernance et la stratégie d'implantation auprès des individus et des entreprises;
  - l'adoption par le Conseil du trésor de la politique gouvernementale de certification incluant notamment les divers éléments d'une politique de sécurité et l'utilisation des extensions des certificats;

- la normalisation d'un certificat à l'usage de l'ensemble du Québec (certificat normalisé);
- l'acquisition et le développement de modules de sécurité;
- l'élaboration d'ententes et d'interfaces sécuritaires.

4.2 Répertoire gouvernemental

L'origine du répertoire gouvernemental est la mesure 5.2 de la politique québécoise de l'autoroute de l'information. Celle-ci s'énonce ainsi : « Voir, de concert avec le ministère des Relations avec les citoyens et de l'Immigration, à mettre en place le répertoire gouvernemental québécois afin de permettre aux individus et aux entreprises d'avoir accès à la description des services offerts à la population, aux références concernant les documents gouvernementaux ainsi qu'aux coordonnées des employés de l'État; le répertoire électronique sera accessible dans le réseau Internet »

Le répertoire gouvernemental s'applique ainsi à l'ensemble des ministères et organismes. Trois fonctions principales y sont associées :

- Localiser : décrire et repérer les objets;
- Garantir : gérer les identités certifiées et les autorisations;
- Partager : soutenir le partage des objets et de leurs divers attributs.

Afin d'atteindre ces objectifs, le SCT publiait en décembre 1997 un rapport intitulé « Conception détaillée du répertoire gouvernemental »[111] ayant pour objet de situer le répertoire gouvernemental dans le contexte du déploiement de l'inforoute et d'illustrer sommairement certaines fonctionnalités. Ce document présente la vue générale du répertoire gouvernemental, l'architecture du service de répertoire, les règles d'appellation et la structure de l'arborescence du répertoire, les mécanismes de sécurité et leur architecture et le schéma du répertoire gouvernemental. On fait état dans ce document des principales classes d'objets à l'intérieur de l'appareil gouvernemental que l'on veut localiser, garantir et partager. À titre d'exemples, on y retrouve les personnes, les unités organisationnelles, les documents, les entités d'application, etc.

La conception du répertoire gouvernemental est sous la responsabilité du SSIGRI du SCT. La DGT est responsable de la mise en œuvre de certains objets et attributs du répertoire alors que la DGSIG apporte un soutien en matière de modélisation des données.

En ce qui concerne les éléments actuellement en place et prévus, on retrouve :

- Au niveau de la fonction localiser, l'utilisation initiale du répertoire est prévue pour la localisation des employés du gouvernement. Un service de répertoire d'une partie des employés du gouvernement est actuellement en hébergement à la DGT. Cette fonction utilise un sous-ensemble de ce répertoire pour donner l'accès aux numéros de téléphone des employés eux-même via l'intranet gouvernemental. Une ouverture éventuelle aux individus via Internet est à l'étude.
- Au niveau de la fonction garantir, l'utilisation du répertoire est prévue initialement pour les fins d'identification et d'authentification ainsi que pour le contrôle des accès des employés du gouvernement devant être connus sur le réseau. À cet effet, le répertoire gouvernemental devient une

[111] On se référera à la *Conception détaillée du répertoire gouvernemental québécois* pour plus de détails sur le site du SCT.

des pièces maîtresses de l'architecture gouvernementale de la sécurité de l'information numérique. Il est prévu que le répertoire gouvernemental soit alimenté et continuellement mis à jour par GIRES. Il est également prévu que la fonction garantir s'appuie sur les résultats des travaux sur l'ICPG au SCT.

- Au niveau de la fonction partage, deux interventions additionnelles associables au répertoire gouvernemental ont été initiées :

  - **l'ingénierie documentaire** : Actuellement une collection de treize documents ont été publiés. La problématique particulière aux documents électroniques a été étudiée et des solutions, des normes et des règles pour répondre aux besoins des organisations ont été mises de l'avant pour la signature et la conservation des documents.
  - **le registre de métadonnées** : Les schémas découlant de l'ingénierie documentaire ont été enregistrés dans un registre de métadonnées.

Il est important de retenir qu'en matière de sécurité de l'information numérique, il existe une relation étroite entre le répertoire, le registre de métadonnées et l'ingénierie documentaire et que l'AGSIN doit en tenir compte (ex. : les règles de sécurité devraient être attachées aux classes XML (schémas) qui sont définies dans le registre de métadonnées ou aux instances de classe qui sont incluses dans le répertoire, etc.).

Le SSIGRI établit actuellement une stratégie afin de compléter un plan d'action pour l'élaboration d'un guide de gestion intégré des documents papiers et électroniques afin d'assister les M/O.

4.2.1 Les orientations du répertoire gouvernemental

Le répertoire gouvernemental est une des pièces essentielles pour répondre aux besoins de l'État-réseau dans le contexte précis du gouvernement. Le répertoire gouvernemental repose sur une organisation de l'information qui en permet la désignation unique et sans ambiguïté, la gestion, le partage et la réutilisation sans oublier les fonctions de sécurité telles que l'identification/authentification et l'habilitation/contrôle d'accès.

La mise en oeuvre du répertoire gouvernemental suppose une technologie appropriée qui s'inscrit dans la philosophie administrative qui prévaut dans l'administration publique québécoise et qui est fondée sur la responsabilisation des ministères et organismes : on parle d'une structure de contrôle répartie à l'échelle de la hiérarchie gouvernementale. S'inspirant des normes internationales de l'ITU[112] (X.500), de l'IETF[113] (Light Directory Access Protocol) et de l'ISO[114] qui marquent le développement des inforoutes sur le plan mondial, le répertoire gouvernemental mise sur l'expérience accumulée dans diverses Administrations.

Il s'appuie aussi sur les analyses du Secrétariat du Conseil du trésor en collaboration avec les organismes concernés afin de proposer une solution concrète aux problèmes de l'Administration québécoise en termes de mise en commun pour le partage et l'exploitation des ressources informationnelles en réseau, et ce dans le respect des mesures de sécurité adéquates.

Le modèle général du répertoire gouvernemental est établi à partir du modèle de répertoire X.500/LDAP, tel que repris à son compte par le monde de l'Internet et tel qu'implanté et commercialisé par les

[112] Union Internationale des télécommunications
[113] Internet Engineering Task Force
[114] Organisation internationale de normalisation

principaux fabricants. Essentiellement, un répertoire X.500/LDAP est constitué d'un ensemble de processus complexes, dont le fonctionnement est réparti pour assurer la prestation et l'administration de services de référence à des ressources en réseau.

De ce point de vue, le répertoire gouvernemental est similaire aux entrepôts de données qui intègrent l'information d'affaires provenant de diverses bases de données avec la principale différence que ce denier a des données stables alors que le répertoire est continuellement sollicité, évolue rapidement et est sujet à des ententes. Du point de vue de l'évolution des systèmes, le répertoire gouvernemental constitue une composante importante de l'évolution des répertoires propriétaires vers des répertoires à base de normes ouvertes.

4.2.2 Les services offerts par le répertoire gouvernemental

Dans le rapport de conception détaillée du répertoire gouvernemental du SCT, différents services ont été identifiés :

- La consultation (analogie aux annuaires téléphoniques);
- Le soutien aux applications (messagerie, sécurité, recherche et publication d'information, etc.).

Les sous-sections qui suivent donnent un aperçu à haut niveau de ces services.

4.2.2.1 Les services de consultation

Les services de consultation (pour la fonction localiser) se subdivisent en quatre services spécifiques soient :

Les services de Pages blanches

- Les Pages blanches fournissent l'information permettant de rejoindre une personne au sein d'un ministère ou d'un organisme (téléphone, adresse, numéro de télécopieur, adresse électronique, etc.) et d'obtenir certains renseignements concernant cette personne.

Les services de Pages bleues

- Les Pages bleues permettent de repérer un ministère ou un organisme à partir de mots-clés décrivant les programmes et les activités de l'organisation. Elles sont aussi destinées à fournir des renseignements sur les structures organisationnelles et les mandats spécifiques des unités administratives.

Les services de Pages vertes

- Les Pages vertes permettent de repérer des informations via des hyperliens avec des sites Web, FTP et autres liens connexes, permettant ainsi d'avoir accès à des documents dans la mesure des restrictions qui s'appliquent selon les lois en vigueur au Québec.

Les services de Pages jaunes

- Les Pages jaunes permettent d'obtenir des renseignements sur certains des fournisseurs qui transigent avec le Gouvernement.

4.2.2.2 Les services de soutien aux applications

Les services de soutien aux applications (pour les fonction garantir et partager) sont :

La messagerie électronique

- Le répertoire gouvernemental supporte l'échange de courrier par messagerie électronique. Il recueille et garde en mémoire les paramètres de messageries électroniques propres aux individus, ministères et organismes, à un groupe, à une liste de distribution, etc.

La sécurité

- Le répertoire gouvernemental se veut un élément fondamental de la sécurité. Il est basé sur la norme/standard X.500/LDAP et offre la capacité d'héberger des certificats de clés publiques basés sur la norme X.509 émis dans le cadre d'une infrastructure à clés publiques permettant notamment la validation des transactions, la sécurité des échanges électroniques et le recours à la signature électronique. Dans une perspective d'État-réseau, le répertoire gouvernemental se confirme facilement dans la catégorie des « meilleures pratiques ».

Applications spécifiques à une organisation

- Le répertoire gouvernemental permet à des ministères et organismes de pouvoir conserver et rendre accessibles des données utilisées par des applications qui leur sont propres.

Autres

- Le répertoire gouvernemental peut soutenir tous les services de différents domaines tels que commerce électronique, Web, Internet et intranet.

4.2.3 La sécurité et le répertoire gouvernemental

Le répertoire gouvernemental vise à répondre aux besoins de sécurité de décrire et repérer les objets, de gérer les identités et les autorisations en plus de soutenir le partage des objets et de leurs divers attributs. Le répertoire gouvernemental est doté de mécanismes de sécurité visant à protéger et à sauvegarder l'information qu'il contient. Il peut aussi contrôler l'accès des utilisateurs et des applications, ainsi que les échanges entre eux. Il est appelé à contenir de plus en plus d'informations précieuses. Sa structure répartie est utile dans la segmentation de l'information et facilite la gestion du contrôle d'accès en fonction d'autorisations définies formellement et avec précision. Un agencement élaboré de concepts, logiciels, procédures administratives et un arrangement de composantes physiques permettent de garantir un degré élevé de sécurité répondant aux plus hautes exigences.

Le répertoire gouvernemental doit être hautement protégé afin de garantir la disponibilité, l'intégrité et la confidentialité des informations numériques emmagasinées, traitées et échangées lors de communications. La conception du répertoire gouvernemental est actuellement sous la responsabilité du SSIGRI du SCT. La DGT assume la réalisation du répertoire alors que la DGSIG apporte un soutien en matière de modélisation des données. Plusieurs considérations en matière de sécurité doivent être couvertes par ces entités afin d'assurer un niveau adéquat de sécurité.

Au niveau juridique, la loi concernant le cadre juridique des technologies de l'information en ce qui a trait à l'utilisation du répertoire pour rendre publics les certificats amènera des obligations qui se traduiront en besoins de sécurité organisationnelle et technologique. À cet effet, les articles 22, 46, 48, 50, 52, 54, 55, 60, 61 et 63 touchent plus particulièrement le répertoire. Les obligations relatives à l'utilisation du service du répertoire pour la publication des certificats et leur vérification devront être garanties par l'organisme responsable du répertoire gouvernemental. De plus, dépendant de la nature des informations numériques emmagasinées, traitées et échangées sur le répertoire, d'autres lois pourraient également préciser des éléments additionnels à considérer.

Du côté humain et organisationnel, certaines responsabilités ne sont pas toutes bien définies ni assumées. La gestion du répertoire nécessitera de définir et de confier un certain nombre de responsabilités de nature commune à un organisme central. Tout comme dans le cas de l'ICPG, il est primordial que les besoins en terme de sécurité administrative et organisationnelle ainsi que du personnel responsable du répertoire soient couverts de manière précise et se reflètent dans une politique de sécurité et un cadre de gestion du répertoire gouvernemental clairement définis. Il en va de même au niveau de la sécurité physique et du milieu ainsi qu'au niveau de la sécurité opérationnelle.

Finalement, au niveau technologique, ces besoins existent principalement au niveau de la normalisation de la configuration et de l'administration sécuritaire du répertoire gouvernemental ainsi que sur la mise en place et la gestion d'outils de prévention, de détection et de correction. De plus, des considérations importantes au niveau des acquisitions et du cycle de développement de systèmes permettront d'assurer au besoin une interopérabilité sécuritaire entre le répertoire gouvernemental et d'autres répertoires de différents paliers gouvernementaux et du secteur privé (domaines de confiance).

4.2.4 L'arrimage avec les infrastructures gouvernementales

4.2.4.1 L'arrimage avec l'ICPG

Dans le cadre de l'AGSIN, il y a nécessité d'utilisation du répertoire gouvernemental pour la publication des certificats de clés publiques des employés de l'état et des mandataires. Il y a un lien étroit entre le répertoire gouvernemental et l'ICPG, dont :

- Les services de répertoire des certificats de clés publiques de l'ICPG pour les employés de l'état et les mandataires en réponse aux utilisateurs et aux applications;
- La liste des certificats révoqués (LCR) pour les employés de l'état et les mandataires dépendant de la politique de confiance et de son pendant de politique de certification qui sera adoptée.

D'autre part, en liaison avec les travaux du certificat normalisé, il est envisagé la mise en place d'un pivot qui aurait notamment pour fonction de constituer et tenir à jour un répertoire des prestataires de services de certification répondant à la norme. Seules les données nécessaires au bon fonctionnement de l'ICPG et pour la validation du certificat normalisé seraient publiées dans ce répertoire.

Ces données sont :

- La liste des certificats croisés des GCC de l'ICPG et des autres autorités de certification avec le pivot;
- La liste des certificats révoqués d'autorités de certification croisés dans l'ICPG.

Par ailleurs, pour fins de validation des certificats de signature des abonnés, le SCT envisage d'utiliser le protocole OCSP, évitant ainsi la consultation massive des listes de certificats révoqués de chaque gestionnaire de clés et certificats.

4.2.4.2 L'arrimage avec GIRES

Dans le contexte actuel, le répertoire gouvernemental est basé sur les normes et standards X.500 et LDAP. Il vise à offrir les services de :

- Pages blanches qui fournissent l'information permettant de rejoindre une personne, plus précisément un employé du gouvernement;
- Pages bleues qui servent à repérer et rejoindre une organisation;
- Pages vertes qui fournissent l'information permettant de repérer un document et d'y avoir accès;
- Pages jaunes qui contiennent les données sur les fournisseurs.

GIRES possède une base d'information potentiellement intéressante pour alimenter le répertoire gouvernemental soit sur les employés du gouvernement, certains employés d'organismes gouvernementaux, certains fournisseurs et équipements du gouvernement.

Les orientations actuelles de la solution GIRES sont à l'effet qu'elle pourrait alimenter le répertoire gouvernemental plus particulièrement des informations de GIRES sur les employés du gouvernement et certains employés d'organismes gouvernementaux. Elle pourrait aussi fournir certaines données sur les fournisseurs qui transigent avec le gouvernement via GIRES.

4.2.5 Concordance du répertoire gouvernemental avec l'AGSIN

Tel que mentionné dans la mise en contexte, le répertoire gouvernemental revêt une importance capitale pour assurer l'identification/authentification et l'habilitation/contrôle d'accès au niveau approprié dans un contexte d'État-réseau. Parmi les utilisations prévues dans le rapport de conception détaillée du répertoire gouvernemental, l'AGSIN a identifié comme potentiel de mise en commun et de partage :

- La répartition (emplacement) sécuritaire et la localisation des informations relatives aux employé(e)s et les certificats de clés publiques associés (incluant LCR);
- La répartition (emplacement) sécuritaire et la localisation des informations relatives aux partenaires/mandataires et les certificats de clés publiques associés (incluant LCR);
- La répartition (emplacement) sécuritaire et la localisation des informations du pivot et les certificats de clés publiques associés (incluant LAR);
- La répartition (emplacement) sécuritaire et la localisation des informations relatives au Registre-référentiel des schémas XML de sécurité normalisés.

L'analyse du rapport de conception détaillée du répertoire gouvernemental confirme que celui-ci est conforme aux principes de l'AGSIN. En ce sens, il respecte les éléments architecturaux de sécurité suivants :

- Basé sur les normes et standards X.500, X.509 et LDAP, il permet entre autres la gestion des informations numériques de :
  - La fonction d'identification/authentification : identifier avec certitude l'utilisateur ou l'application qui demande l'accès;
  - La fonction d'habilitation/contrôle d'accès : permettre aux détenteurs d'information contenue dans la base des entrées de limiter l'accès et de restreindre les opérations effectuées sur les entrées.

- Les concepts de sécurité avancés en vue de garantir la sécurité des ressources et des échanges en réseau sont ceux de la norme ISO 7498-2 retenue dans le cadre de l'AGSIN qui définit le fonctionnement en réseau soit :
  - **Habilitation/contrôle d'accès** : déterminer les données et applications qu'un utilisateur authentifié est autorisé à consulter, modifier, etc.;
  - **Identification/authentification** : déterminer qui se connecte à un serveur donné et son identité véritable;
  - **Confidentialité** : garantir la confidentialité des informations et sa non-accessibilité;
  - **Intégrité** : garantir que les données n'ont pas été modifiées lors de leur transmission ou depuis leur dernière mise à jour;
  - **Irrévocabilité** : garantir que le destinataire ne pourra nier avoir reçu un message ou l'émetteur de l'avoir transmis.

4.2.6 Conclusion

La documentation et les consultations n'ont pas permis d'identifier de manière spécifique les éléments de stratégie et de planification d'ensemble pour la poursuite des travaux qui concernent le répertoire gouvernemental. Les travaux relatifs à ce dernier s'exécutent actuellement selon une approche expérimentale.

En conclusion, l'hypothèse suivante est proposée:

GIRES traite des informations potentiellement intéressantes pour alimenter le répertoire gouvernemental soit sur les employés du gouvernement, certains employés d'organismes gouvernementaux, certains fournisseurs et des équipements du gouvernement.

Le répertoire gouvernemental pourrait s'alimenter plus particulièrement des informations de GIRES sur les employés du gouvernement, certains employés d'organismes gouvernementaux et de certains fournisseurs du gouvernement.

Le constat selon cette hypothèse :

Il est réaliste d'utiliser le répertoire gouvernemental comme élément fondamental de la sécurité pour assurer, au besoin, l'identification/authentification et l'habilitation/contrôle d'accès. Le répertoire

gouvernemental, du moins dans sa définition[115], rencontre les concepts mis de l'avant par l'AGSIN. Il répond aux rôles qui pourraient être dévolus à un répertoire dans l'architecture cible. Toutefois, certains éléments, notamment reliés à la gouvernance, doivent être établis avant d'utiliser le répertoire gouvernemental comme assise à la sécurité.

Pour ce faire, les travaux suivants devraient être réalisés :

- Identifier les autres sources qui pourront compléter les informations de sécurité fournies par GIRES ainsi que les autres services potentiels du répertoire gouvernemental de manière à permettre à ce dernier de remplir pleinement son rôle sur la sécurité.
- Définir une politique de sécurité et un cadre de gestion de sécurité propres au répertoire gouvernemental étant donné son implication dans l'AGSIN.
- Définir clairement les rôles et les responsabilités :
  - Il y aura lieu de réaliser des travaux d'architecture de l'information (hiérarchisation) gouvernementale et de définir concrètement les rôles et les responsabilités (propriétaire et détenteur de l'information) et les processus qui supporteront ces rôles et responsabilités.
- Élaborer une stratégie et une planification d'ensemble intégrant l'utilisation du répertoire, du registre des métadonnées et de l'ingénierie documentaire. L'utilisation ou non d'un répertoire gouvernemental amènera aussi plusieurs enjeux tels que :

Non-utilisation	Utilisation
➢ Réplications multiples des profils d'utilisateurs; ➢ Multiples modèles de sécurité; ➢ Complexité accrue au niveau de la gestion.	➢ un seul profil pour chaque utilisateur; ➢ un seul modèle de sécurité; ➢ une complexité moindre au niveau de la gestion; ➢ une réduction des coûts d'application de la sécurité.

- Des travaux subséquents restent également à être complétés, soit principalement au niveau de :
  - l'acquisition et le développement de modules de sécurité propres au répertoire;
  - l'élaboration d'ententes et d'interfaces sécuritaires propres au répertoire;
  - l'élaboration d'un guide de gestion intégrée des documents couvrant bien l'aspect sécurité.

4.3 La solution GIRES

Amenés par la loi sur l'administration publique à se pencher sur l'efficacité et la performance de leurs organisations, les M/O doivent se munir d'outils permettant une meilleure gestion de leurs ressources. C'est dans cette perspective que le Conseil du trésor a autorisé, en février 1999, le lancement d'un appel d'offres en vue d'acquérir un progiciel de gestion intégrée des ressources humaines, financières et matérielles. Avec l'aide des ministères et organismes, le gouvernement a arrêté son choix en juin 1999 sur le progiciel de la firme Oracle.

[115] *Conception détaillée du répertoire gouvernemental québécois*, Conseil du trésor

La solution GIRES vise à implanter un ensemble d'applications en ressources humaines, financières et matérielles faisant partie du progiciel intégré du fournisseur Oracle. Principalement, GIRES est appelé à remplacer SAGIP (Système automatisé de gestion des informations sur le personnel) et SYGBEC (Système de gestion budgétaire et comptable). Cette solution prévoit introduire des facilités administratives axées sur les méthodes les plus modernes de gestion au gouvernement du Québec. La solution GIRES offrira les services suivants :

La solution GIRES – ressources humaines

Les fonctionnalités de gestion des ressources humaines et de la paie pour supporter la *Loi sur la fonction publique* et la réglementation afférente aux organismes dont le personnel est nommé ou rémunéré en vertu de cette loi.

La solution GIRES – ressources financières

Les fonctionnalités nécessaires aux opérations financières et au suivi budgétaire prévus par la *Loi sur l'administration financière*, la *Loi sur le ministère des finances*, la *Loi sur l'administration publique* et la réglementation afférente.

La solution GIRES – ressources matérielles

Les fonctionnalités nécessaires à l'application de la *Loi sur l'administration financière*, la *Loi sur le service des achats du gouvernement*, la politique sur les marchés publics et la réglementation afférente.

4.3.1 Les systèmes et interfaces visés

Outre les systèmes SAGIP et SYGBEC, un ensemble d'interfaces sont touchés par la solution GIRES. Les interfaces touchées sont en provenance ou à destination de SAGIP et SYGBEC. Elles peuvent être catégorisés comme suit :

- Les interfaces avec les systèmes des partenaires externes tels que certains organismes non assujettis à la *Loi sur la fonction publique*, les institutions bancaires, trusts, fonds, compagnies d'assurance, syndicats, etc.;
- Les interfaces avec les systèmes de mission des ministères et organismes.

Les interfaces entre SAGIP et SYGBEC et les systèmes périphériques qui seront remplacées par GIRES sont : SAGIP, SYGBEC, SIGMA, GAAS, SADE, SDE, GEO, GRIEF, Dotation (faible volume), Dotation, MEDIA, Formel, Emmanuel, SIPB, États financiers, le Centre d'Information, Interrogation des listes, Impression destinataire, Impression rapports et Mirage.

4.3.2 Les clientèles

Les clientèles de la solution GIRES se composent de près de 66 000 utilisateurs répartis dans 156 ministères, organismes ou fonds spéciaux. Les utilisateurs réguliers sont estimés à environ 11 000, dont 3 875 gestionnaires.

La solution GIRES vise donc différentes clientèles qui peuvent se subdiviser en deux (2) groupes.

Le premier groupe : La plupart des ministères et organismes du gouvernement du Québec

- Tout ministère et organisme assujetti à la « Loi sur la fonction publique » devra utiliser la « solution GIRES » en matière de ressources humaines;
- Tout ministère et organisme du gouvernement dont le budget est voté ainsi que tous fonds spéciaux ayant sa propre entité comptable devront utiliser la « solution GIRES » en matière de ressources financières et matérielles.

Le deuxième groupe : La clientèle potentielle

Elle se compose d'organismes possédant une plus grande autonomie au sein de l'appareil gouvernemental quant à leur budgétisation et à la gestion de leur finance, mais qui sont soumis aux mêmes règles de gestion que les M/O selon la *Loi sur la fonction publique*. Les organismes faisant partie de la clientèle potentielle sont, par exemple :

- Commission administrative des régimes de retraite et d'assurance;
- Commission des normes du travail;
- Commission de la santé et de la sécurité du travail;
- Régie de l'assurance-maladie du Québec;
- Régie des rentes du Québec;
- Société de l'assurance-automobile du Québec.

4.3.3 La sécurité et la solution GIRES

La solution GIRES prévoit mettre en place tous les mécanismes de sécurité pertinents supportant les fonctions[116] de sécurité nécessaires pour la protection de ses modèles d'affaires (ressources humaines, financières, matérielles), des renseignements personnels et des informations confidentielles et stratégiques selon les lois et règlements en vigueur[117].

Selon les travaux planifiés[118] actuellement, les éléments de sécurité de la solution GIRES visent à protéger ses propres informations numériques en regard de :

- L'étendue (les clientèles visées) et la diversité de leurs structures organisationnelles;
- Les échanges d'informations entre les organisations;
- Les arrimages à réaliser avec les différents systèmes ministériels (les interfaces);
- L'inforoute gouvernementale;
- L'utilisation intensive de plusieurs nouvelles technologies.

[116] On se référera à la section 2.5 pour plus d'informations sur les mécanismes de sécurité et les fonctions de sécurité.
[117] On consultera la section 1.4 pour plus d'informations
[118] On consultera l'appel d'offres de la solution GIRES, p.408-409, pour plus de détails.

La solution GIRES vise aussi à mettre en place tous les processus[119] nécessaires à son fonctionnement y compris celui de la gestion de la sécurité. Ce processus spécifique assurera que la solution GIRES fonctionnera :

- en conformité avec le cadre légal et réglementaire en vigueur en regard de la protection des renseignements personnels et confidentiels, des droits d'auteur et du respect de la vie privée;
- dans un environnement assurant l'intégrité des applications et des outils utilisés;
- en assurant l'intégrité des données traitées et conservées durant tout le cycle de vie de celles-ci;
- en protégeant les actifs informationnels composant sa solution (matériel, logiciels, données et intervenants).

La mise en place des processus de la solution GIRES aura cependant des impacts sur la sécurité dans les ministères et organismes utilisateurs de la solution. Elle amènera des changements qui, en version préliminaire, ont été identifiés comme :

- le partage des responsabilités en matière de sécurité de l'information entre plusieurs partenaires (SSGIR et M/O) (notion de propriété);
- l'uniformisation des politiques de sécurité et leur application;
- le remplacement des contrôles actuellement manuels par des contrôles informatisés;
- le haut niveau de sécurité nécessaire compte tenu de la forte concentration de données nominatives et confidentielles dans une même banque;
- une gestion des accès plus complexe nécessitant des moyens plus robustes.

Dans le contexte actuel, la solution GIRES a pris en compte ou couvert dans la nomenclature des travaux qui seront réalisés, tous les éléments de manière à assurer la sécurité de l'informaton numérique et des échanges électroniques qui seront concernés conformément à l'AGSIN. Cependant, comme GIRES servira à centraliser les données relatives aux ressources du gouvernement, et non simplement à aiguiller les requêtes, il est de la plus grande importance de lui accorder un très haut niveau d'attention et de protection.

Au niveau juridique, GIRES doit tenir compte des différentes lois et règlements régissant l'administration publique, particulièrement la loi 82, et la loi concernant le cadre juridique des technologies de l'information. Notons que GIRES considérera tout autant l'opportunité et la pertinence de procéder à des ajustements du cadre réglementaire que la modification des pratiques d'affaires éprouvées incluses dans le progiciel.

D'un point de vue humain et organisationnel, de nombreuses mesures sont nécessaires :

- Des éléments encadrants tels que des politiques, directives et procédures de sécurité spécifiques à GIRES devront aussi être développées ;
- Une définition des responsabilités respectives des M/O et de GIRES en matière de sécurité de l'information est nécessaire. Des efforts importants ont déjà été consentis à ce niveau ;

[119] On consultera l'appel d'offres de la solution GIRES, p.409, pour plus d'informations.

- La définition des rôles et responsabilités en matière de sécurité est nécessaire à la fois dans les M/O et dans GIRES ;
- La mise en place d'un cadre de gestion de l'exploitation, de procédures de surveillance, d'un plan de relève, d'un plan d'urgence, etc., sont nécessaires ;
- Les infrastructures technologiques devront être hébergées dans un centre où l'accès sera contrôlé. Cela fera donc en sorte que des mesures seront en place et ainsi d'un point de vue sécurité physique tous les équipements feront l'objet d'une protection.

Du côté technologique, GIRES doit se protéger contre les intrusions. Ainsi, il est prévu qu'il utilise les différents coupe-feu de la DGSIG. Afin de protéger le trafic, les échanges entre les postes de travail et les serveurs de GIRES seront cryptés et les transactions devront s'effectuer uniquement sur un réseau privé protégé de l'Internet. De plus, un accès à distance (RAS) à partir d'un modem ou un accès Internet sécurisé (RPV, par exemple) devra permettre aux utilisateurs en mode libre-service de se brancher sécuritairement au réseau à partir de l'extérieur. Ces derniers besoins correspondent en partie aux services offerts par le RICIB et aux services qui seront offerts par le RETEM.

Il est aussi prévu que GIRES utilisera le chiffrement des messages et implantera la sécurité définie dans les applications Oracle pour identifier/authentifier et habiliter/contrôler les accès de tous les utilisateurs avant de leur donner accès à GIRES, et ce, en fonction des droits d'accès qui leur ont été accordés. La méthode d'identification/authentification supportée pour le moment est l'utilisation d'un code utilisateur et d'un mot de passe (authentification faible). Cependant, l'utilisation d'une méthode d'authentification forte est à l'étude. Deux méthodes sont étudiées, l'utilisation d'un jeton d'authentification ou d'un certificat. Dans ce dernier cas, il est nullement prévu que GIRES déploie sa propre ICP. Notons que l'utilisation d'une ICP se fera conjointement avec la fonction de sécurité de Oracle.

Au niveau de la disponibilité, il est impératif que GIRES soit hautement disponible en période d'exploitation puisqu'il sera le centre névralgique de la gestion des ressources au gouvernement du Québec. Des mécanismes robustes devront être utilisés : mécanismes de duplication et de redondance des infrastructures technologiques, applications et informations numériques, balancement de la charge, outils d'exploitation pour assurer un suivi automatisé et serré de l'environnement, etc.

4.3.4 L'arrimage avec les infrastructures gouvernementales

4.3.4.1 L'arrimage avec l'ICPG

Telle que définie dans la solution GIRES, l'utilisation de l'ICPG est associée aux pages blanches du répertoire gouvernemental en ce qui concerne les employés de l'état. L'ICPG pourrait permettre, par la gestion des clés publiques et l'émission des certificats, d'assurer :

- L'identification/authentification ;
- L'habilitation/contrôle d'accès ;
- La confidentialité ;
- L'intégrité ;
- L'irrévocabilité.

Les orientations de la solution GIRES précisent que, à prime abord, GIRES n'a pas besoin d'une ICP. Selon le sous-secrétariat à la gestion des ressources, la solution pourrait très bien fonctionner à l'aide de l'authentification disponible avec Oracle, à savoir un code d'utilisateur et un mot de passe avec chiffrement de l'information lors des communications. Toutefois, les orientations gouvernementales en matière de sécurité de l'information et des échanges électroniques font en sorte qu'il soit probable qu'une ICP soit nécessaire à la solution GIRES dans un mode de fonctionnement sans papier.

Pour l'instant, l'orientation retenue préconise l'utilisation des fonctions de base de sécurité fournies avec Oracle et de réaliser les analyses plus poussées afin d'établir si l'utilisation de certificats de clés publiques, de chiffrement ou autres seront nécessaires pour certaines des transactions de la solution GIRES. La firme Oracle doit fournir à la solution GIRES toutes les fonctionnalités relatives à l'ICP avec la version 11i.3 . Toutefois, Oracle et ENTRUST (fournisseur actuel du service de gestion de clés et certificats de la DGT dans le cadre de l'ICPG) ne peuvent confirmer la date à laquelle le lien Oracle/ENTRUST sera disponible.

4.3.4.2 L'arrimage avec le répertoire gouvernemental

Dans le contexte actuel, le répertoire gouvernemental est basé sur les normes et standards X.500 et LDAP. Il vise à offrir les services de :

- Pages blanches qui fournissent l'information permettant de rejoindre une personne, plus précisément un employé du gouvernement;
- Pages bleues qui servent à repérer et rejoindre une organisation;
- Pages vertes qui fournissent l'information permettant de repérer un document et d'y avoir accès;
- Pages jaunes qui contiennent les données sur les fournisseurs.

GIRES possède une base d'information potentiellement intéressante pour alimenter le répertoire gouvernemental soit sur les employés du gouvernement, certains employés d'organismes gouvernementaux, certains fournisseurs et équipements du gouvernement.

Les orientations actuelles de la solution GIRES sont à l'effet qu'elle pourrait alimenter le répertoire gouvernemental plus particulièrement des informations sur les employés du gouvernement et certains employés d'organismes gouvernementaux. Elle pourrait aussi fournir certaines données sur les fournisseurs qui transigent avec le gouvernement via GIRES.

4.3.5 Concordance de GIRES avec l'AGSIN

Dans une optique d'architecture gouvernementale de la sécurité de l'information numérique, GIRES aura un rôle important. En effet, le répertoire gouvernemental est une des pièces maîtresse de l'architecture gouvernementale de la sécurité de l'information numérique et il est nécessaire que GIRES l'alimente et le mette continuellement à jour.

L'architecture gouvernementale de sécurité de l'information numérique propose un ensemble de fonctions et de mécanismes de sécurité afin d'assurer la protection de l'information numérique et des échanges électroniques, appuyés par le concept de domaines de confiance. Dans les travaux planifiés à ce jour, la solution GIRES couvre toutes les fonctions soient :

- Intégrité;
- Irrévocabilité;
- Identification/Authentification;
- Habilitation/Contrôle d'accès;
- Confidentialité;
- Disponibilité;
- Surveillance;
- Administration.

La solution GIRES prévoit réaliser les travaux relatifs à la catégorisation de son information numérique de manière à la sécuriser selon le niveau de la valeur établie.

4.3.6 Conclusion

La conclusion propose l'hypothèse suivante :

La solution GIRES est le principal fournisseur du répertoire gouvernemental quant aux informations sur les employés du gouvernement, certains employés d'organismes gouvernementaux et certains fournisseurs du gouvernement.

Le constat selon cette hypothèse

Il est tout à fait réaliste de penser utiliser GIRES comme principal fournisseur d'informations sur certaines catégories d'employés et de fournisseurs pour alimenter le répertoire gouvernemental afin de supporter les fonctions de sécurité reliées à l'identification/authentification et à l'habilitation/contrôle d'accès.

Pour ce faire, certaines activités spécifiques devront cependant être réalisées. Notamment :

- Réviser les pratiques à être centralisées et décentralisées :
  - La solution GIRES modifiera certaines façons de faire actuelles en matière de pratiques de gestion dans tous les M/O. Certaines pratiques devront êtres décentralisées notamment celles visant à accroître l'autonomie des gestionnaires et d'autres, centralisées afin d'accroître l'autonomie des clientèles (guichet unique).
  - Ces pratiques devront faire l'objet d'analyses de manière à bien identifier la valeur ajoutée et les enjeux en matière de sécurité.
- Revoir le partage des responsabilités (gouvernance)
  - Il sera fondamental d'identifier les propriétaires et les détenteurs de l'information ainsi que les processus qui les supportent, en lien avec les pratiques centralisées et décentralisées qui seront proposées. Le nouveau partage des responsabilités permettra de consolider le rôle de la solution GIRES et aussi du répertoire gouvernemental en matière de sécurité de l'information numérique et des échanges électroniques. Une gouvernance adaptée à la nouvelle réalité gouvernementale facilitera grandement cette tâche.
- Définir une politique de sécurité et un cadre de gestion de sécurité de façon adéquate à GIRES étant donné le potentiel d'utilisation de la base d'information de GIRES identifié dans l'AGSIN;

- Élaborer un guide de développement de modules de sécurité de façon adéquate à GIRES afin de ne pas affaiblir le niveau de protection prévue de GIRES;
- Élaborer des ententes et interfaces sécuritaires facilitant l'utilisation sécuritaire de GIRES;
- Examiner l'utilisation des composantes communes de sécurité envisagées par le gouvernement;
- Tenir compte de l'architecture cible de l'AGSIN dans son développement.

4.4 Le RICIB et le RETEM

La Direction générale des télécommunications est l'une des constituantes du Sous-secrétariat aux services gouvernementaux. Elle développe et fournit à l'appareil gouvernemental des produits et services de télécommunications, en s'appuyant sur des partenariats d'affaires avec divers intervenants du secteur privé. Dans l'accomplissement de son mandat, la DGT identifie les besoins des ministères et organismes clients par l'analyse de leurs profils d'activités et s'appuie sur le recours à la concurrence pour leur procurer les meilleurs produits et services au meilleur coût. De plus, elle agit à titre conseil auprès du gouvernement pour le développement et l'exploitation intégrée des infrastructures et des réseaux de télécommunications. Elle assume également une responsabilité dans la gestion des crises et des urgences, suite à une réorganisation de la Sécurité civile. L'une des offres principales de la DGT est un réseau intégré de communications, le RICIB.

Considérant la demande mettant de plus en plus à l'épreuve les capacités du RICIB et la fin du contrat en cours, le RICIB sera remplacé par un réseau de plus grande capacité, le Réseau de télécommunication multimédia de l'administration publique québécoise (RETEM). Le RETEM vise à soutenir de façon plus efficace et à moindre coût le déploiement des services électroniques par les ministères et organismes en fournissant notamment des services réseaux, des services Internet et intranet et des services de téléphonie à l'ensemble des M/O, à l'exception des sociétés d'État à vocation commerciale. Celles-ci pourront cependant, le cas échéant, recourir aux services rendus disponibles par ce réseau. Plus spécifiquement, le RETEM vise à :

- Reconduire les fonctionnalités (incluant les éléments de sécurité) du RICIB ;
- Augmenter la bande passante ;
- Offrir des fonctionnalités de « Qualité de services » (QoS);
- Inclure les fonctionnalités de l'Internet;
- Inclure la téléphonie.

4.4.1 Positionnement du RICIB et du RETEM

Le RICIB, qui constitue actuellement l'ossature de base de l'inforoute gouvernementale, est un réseau porteur à capacité étendue, basé sur la technologie Magellan et sur la technologie des routeurs. Il est constitué de nœuds intelligents et partagés de télécommunication qui sont reliés par des liaisons numériques à large bande. Ces nœuds de réseau sont localisés dans des points régionaux sélectionnés en fonction d'une répartition optimale des coûts et de la performance. À partir de ces points, le RICIB rayonne par le biais de liaisons d'accès sur toutes les villes du Québec et rend disponible une gamme de services.

En plus de fournir des services d'accès aux banques d'information, de maillage des réseaux locaux, d'accès à un ensemble de services spécialisés de l'inforoute gouvernementale, de communication entre les

réseaux des ministères et les réseaux publics et de distribution d'informations de gestion de réseau, le RICIB fournit à ses abonnés la possibilité de configurations spéciales en fonction d'effectuer des transactions avec le niveau de sécurité approprié à la confidentialité des données qui sont échangées.

De son côté, l'infrastructure du RETEM, centré sur un réseau IP, couvrira la presque totalité du territoire du Québec et permettra l'interconnexion avec des réseaux externes pour étendre sa portée sur le plan mondial. De plus, des passerelles de communication seront établies entre le RETEM et les grands réseaux publics gouvernementaux dans les secteurs de la santé (RTSS) et de l'Éducation (RISQ).

4.4.2 La sécurité et le RICIB et le RETEM

Étant l'épine dorsale (un élément commun) des échanges électroniques au gouvernement du Québec, le RICIB (et son remplaçant le RETEM) sert au transit d'informations de toutes valeurs et se doit donc d'être hautement protégé en tout temps. Une cueillette auprès de la DGT a permis d'établir qu'elle offre les mécanismes et éléments de sécurité suivants à ses clients :

- Redondance des infrastructures à Québec et Montréal ;
- Cloisonnement (circuit virtuel) du trafic des M/O sur les routeurs dédiés et partagés ;
- Coupe-feu (passerelles de sécurité) pour le filtrage des adresses et des protocoles ;
- Création de périmètres de sécurité;
- Journalisation de ce qui transite par les périmètres;
- Détection des tentatives d'intrusions au niveau des serveurs et applications hébergés dans la zone démilitarizée Internet ;
- Services Réseau Privé Virtuel.

Tel que nous l'avons vu aux sections 2.5 et 2.6, plusieurs mécanismes et solutions technologiques sont nécessaires afin de garantir un niveau élevé des attributs de sécurité DICAI étendu (DICAI auquel on ajoute les trois autres fonctions). Outre les mécanismes listés plus hauts, le RICIB (et son remplaçant le RETEM) doit compter sur de nombreux éléments de sécurité. Selon les informations disponibles sur le RICIB, il apparaît clairement qu'un certain nombre d'améliorations en matière de sécurité devront être prises en considération pour le RETEM. Mentionnons notamment des améliorations au niveau des éléments suivants[120] :

Dimension organisationnelle :

- Rôles et responsabilités du personnel chargé de la sécurité ;
- Politiques, normes et directives de sécurité spécifiques à la sécurisation du réseau, incluant une politique d'interconnexion entre le RICIB, le RETEM et les réseaux des M/O et secteurs de la santé, de l'Éducation et municipal (RTSS et RISQ);
- Guides et procédures de sécurité ;
- Évaluation de vulnérabilités ;

[120] Certains de ces éléments sont déjà en place mais nécessitent des améliorations. D'autres ne sont pas en place. Pour des raisons de sécurité, aucun détail supplémentaire ne sera donné ici.

- Plan d'urgence, de relève et de continuité ;
- Audits ;
- Contrôle de l'accès physique ;
- Accès aux serveurs et équipements ;
- Mesures d'urgences;
- Gestion des changements.

Dimension technologique :

- Systèmes d'exploitations sécurisés ;
- Coupe-feu (passerelles de sécurité);
- Redondance physique et des fournisseurs de services ;
- Outils d'administration des logiciels et équipements réseau ;
- Analyseur de vulnérabilités sur le réseau et sur les serveurs ;
- Moniteur de contenu actif ;
- Outil de surveillance réseau ;
- Sondes de détection;
- Détection des tentatives d'intrusions sur le réseau et serveurs associés;
- Détection de virus sur la transmission de courrier ;
- Accès à distance chiffré (RPV, SSH, SSL, ICP).

4.4.3 Concordance du RICIB et du RETEM avec l'AGSIN

Le RICIB (et son remplaçant le RETEM) est au cœur de la vue infrastructure technologique et peut être considéré comme une composante commune à l'ensemble du gouvernement du Québec. Les mécanismes et solutions technologiques de sécurité déployés sur celui-ci peuvent donc être considérés eux-mêmes comme des composantes communes qui assurent la sécurité du transport des informations.

Rappelons que les diverses composantes communes, partagées et réutilisables potentielles qui ont trait au RICIB (et son remplaçant le RETEM) ont été identifiées à la section 2.7.

5. ZONES ET OBJETS DE NORMALISATION

Cette section identifie des zones et objets de normalisation potentiels ainsi que des normes ouvertes, de jure, de facto ou émergentes pertinentes aux différents volets du modèle général de l'AGSIN. Ces zones et objets de normalisation peuvent s'appliquer à des documents, des règles, des critères, des mécanismes de sécurité, des solutions technologiques ou des processus.

Notons que les normes et standards dominants les plus pertinents à chaque zone et objet de normalisation sont identifiés. Une description de ces normes et standards se situe à l'annexe D.

5.1 Volet affaires

Afin de faciliter l'évaluation de la sécurité des domaines de confiance et assurer une cohérence et une uniformité gouvernementales envers les clientèles, les zones et objets de normalisation suivants sont identifiés :

- Normaliser, au niveau gouvernemental québécois, le format et le contenu des politiques de sécurité :
  - Normes et standards dominants pertinents : ISO/IEC 17799, Manuel canadien de la sécurité des technologies de l'information
- Normaliser, au niveau gouvernemental québécois, le format et le contenu des cadres de gestion de la sécurité [121]:
  - Normes et standards dominants pertinents : ISO/IEC 13335
- Normaliser, au niveau gouvernemental québécois, les ententes et les interfaces sécuritaires des composantes communes :
  - Normes et standards dominants pertinents : aucun
- Normaliser, au niveau des grappes de services et au niveau sectoriel, les ententes et les interfaces sécuritaires des composantes partageables :
  - Normes et standards dominants pertinents : aucun
- Normaliser, au niveau gouvernemental québécois, le mode d'établissement des ententes et interfaces sécuritaires (guides) avec les clientèles et les M/O

5.2 Volet information

Afin de favoriser les échanges d'informations numériques sécuritaires entre les domaines de confiance et avec les clientèles, les zones et objets suivants de normalisation sont identifiés en ce qui concerne l'information de sécurité :

- Normaliser, au niveau gouvernemental québécois, la catégorisation de l'information numérique et la méthodologie d'évaluation des menaces et des risques :

[121] Le SCT a déjà entrepris cette normalisation puisque son Modèle de gestion de la sécurité des systèmes d'information dans l'Administration publique est basé sur la norme 13335.

  - Normes et standards dominants pertinents : Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité

- Normaliser, au niveau gouvernemental québécois, les schémas de métadonnées XML de sécurité des composantes partageables :
  - Normes et standards dominants pertinents : ebXML (XML, XML Signature, XML Encryption, XML Schema)
- Normaliser, au niveau québécois, les formats et les contenus des clés et des certificats de même que la délivrance et la gestion des certificats :
  - Normes et standards dominants pertinents : certificat X.509 de l'UIT, certificat WTLS du WAP Forum
- Normaliser les informations communes relatives à la sécurité (ex : localisation des employés)
- Normaliser, au niveau gouvernemental québécois, les règles de surveillance et de définition spécifiques
  - Normes et standards dominants pertinents : aucun

5.3 Volet application

Afin d'assurer une sécurité adéquate et de permettre un maximum d'interopérabilité, les zones et objets suivants de normalisation sont identifiés en ce qui concerne les applications et modules de sécurité :

- Normaliser les critères de sélection en matière de sécurité pour l'acquisition des applications (de sécurité ou des composantes de sécurité des autres) et des modules de sécurité
  - Normes et standards dominants pertinents : « Critères communs » ou ISO/IEC 15408
- Normaliser les critères de développement en matière de sécurité des applications et des modules de sécurité
  - Normes et standards dominants pertinents : « Critères communs » ou ISO/IEC 15408
- Identifier les normes recommandées au niveau gouvernemental québécois pour les mécanismes de sécurité et solutions technologiques (volet application)
  - Normes et standards dominants pertinents : X.500 de l'UIT, LDAP, PKIX de l'IETF, PKCS de RSA, SSL/TLS de l'IETF, WTLS du WAP Forum, SNMP

5.4 Volet infrastructure technologique

Afin d'assurer un niveau adéquat de disponibilité, d'intégrité et de confidentialité, les zones et objets suivants de normalisation sont identifiés :

- Normaliser les critères de sélection en matière de sécurité pour l'acquisition d'infrastructure technologique de sécurité
  - Normes et standards dominants pertinents : « Critères communs » ou ISO/IEC 15408
- Normaliser les processus d'installation, de paramétrisation et de sécurisation
  - Normes et standards dominants pertinents : Guides spécifiques

- Identifier les normes recommandées au niveau gouvernemental québécois pour les mécanismes de sécurité et solutions technologiques (volet infrastructure technologique)
  - Normes et standards dominants pertinents : IPSec

6. EXEMPLES DE SCÉNARIOS D'UTILISATION

Cette section présente des exemples (scénarios) d'application des concepts de l'AGSIN. Ceux-ci ont été élaborés afin de supporter les ministères et organismes dans leur compréhension de l'AGSIN. Ils illustrent, à l'aide d'exemples clairs et simples, l'interrelation entre l'information catégorisée, les fonctions de sécurité et les mécanismes qui s'y rattachent (voir tableau à la section 2.6.2) afin de protéger l'information numérique et les échanges électroniques.

Par exemple, un scénario illustrera une situation de service hypothétique telle que :

- pour protéger l'échange d'une information nominative ou personnelle entre deux M/O, la protection accordée à l'information transmise électroniquement pourrait nécessiter une authentification élevée (forte) qui devrait être supportée par des mécanismes tels que le jeton ou le certificat de clés publiques de signature et un mot de passe.

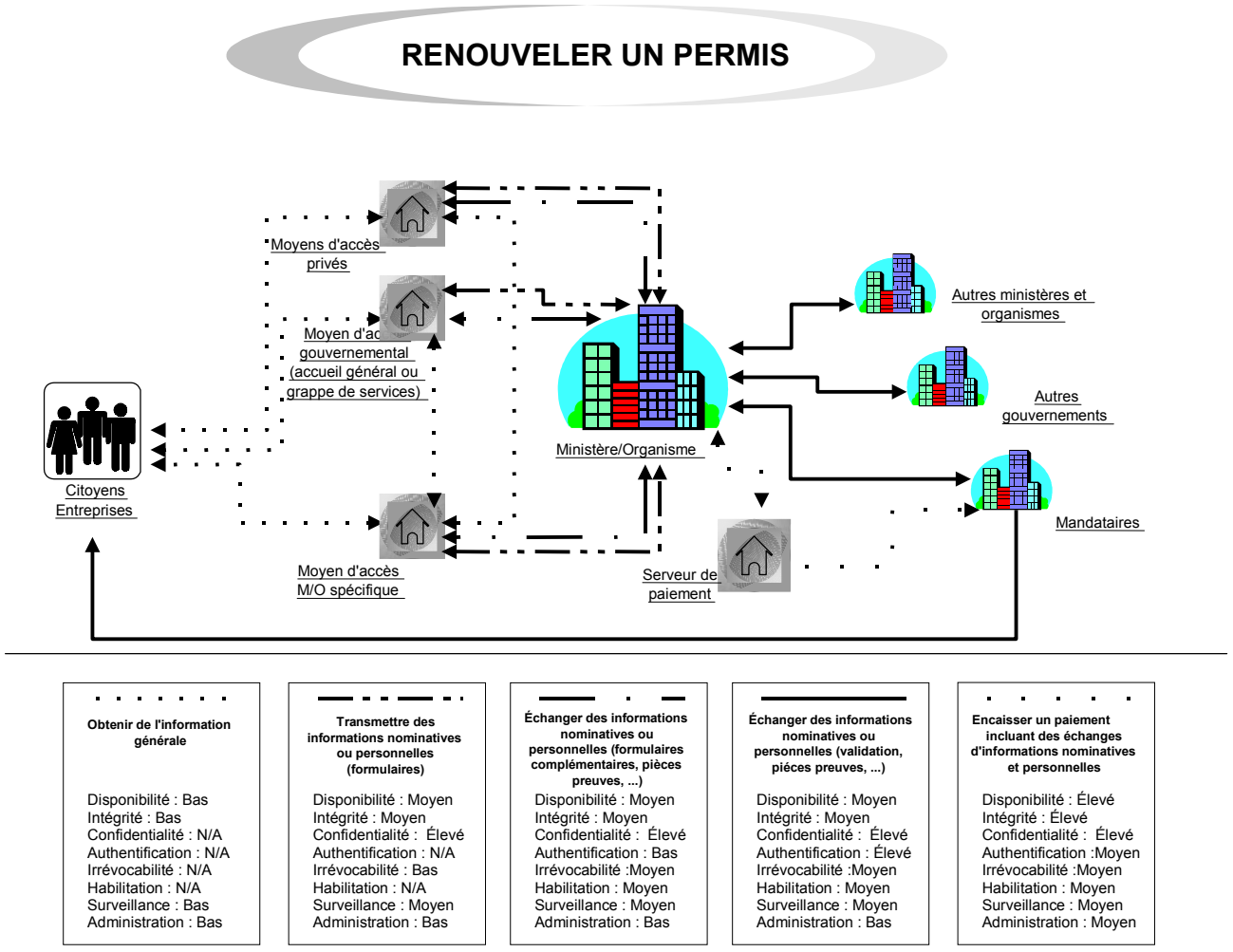
Il est important de souligner que les scénarios ne prétendent pas décrire de manière exacte le processus d'une prestation électronique de services particulière. Tel que précisé précédemment, ils ont été élaborés à titre indicatif pour illustrer l'application des concepts de l'AGSIN à haut niveau. Ces scénarios présentent des cas où l'individu ou l'entreprise transige de manière électronique avec l'Administration publique en respectant les concepts de l'architecture d'entreprise gouvernementale[122]. Dans ce contexte, rappelons que l'individu ou le représentant de l'entreprise peut accéder par différents moyens pour obtenir une prestation électronique de services.

Trois scénarios sont illustrés en utilisant les symboles suivants :

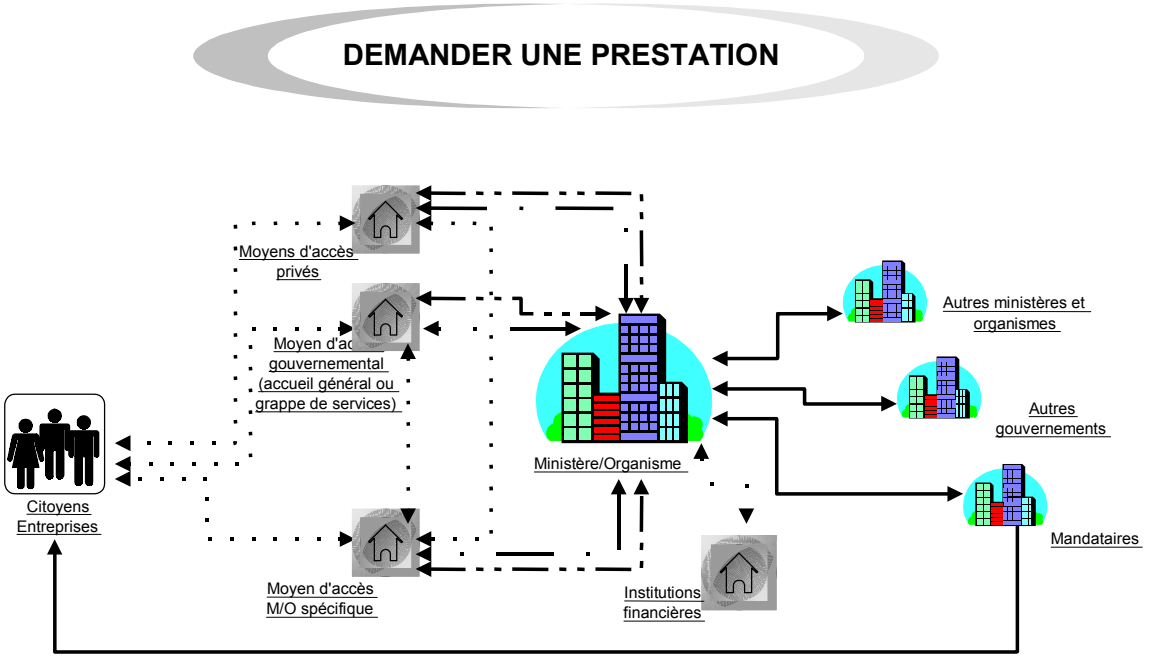
	Individus/Entreprises
	Moyens d'accès (privés, gouvernemental ou d'un ministère et organisme spécifique)
	Organisations (ministère, organisme, mandataire, gouvernement, partenaire)
Traits de diverses formes	Liens d'affaires selon le type d'information numérique échangé (information générale, renseignements nominatifs ou confidentiels)

[122] On consultera le document *Architecture d'entreprise gouvernementale – Contexte, perspectives et architecture de haut niveau* pour plus de détails.

6.1 Renouveler un permis



6.2 Demander une prestation



Obtenir de l'information générale

Disponibilité : Bas
Intégrité : Bas
Confidentialité : N/A
Authentification : N/A
Irrévocabilité : N/A
Habilitation : N/A
Surveillance : Bas
Administration : Bas

Transmettre des informations nominatives ou personnelles (formulaires)

Disponibilité : Moyen
Intégrité : Moyen
Confidentialité : Élevé
Authentification : N/A
Irrévocabilité : Bas
Habilitation : N/A
Surveillance : Moyen
Administration : Bas

Échanger des informations nominatives ou personnelles (formulaires complémentaires, pièces preuves, ...)

Disponibilité : Moyen
Intégrité : Moyen
Confidentialité : Élevé
Authentification : Bas
Irrévocabilité :Moyen
Habilitation : Moyen
Surveillance : Moyen
Administration : Bas

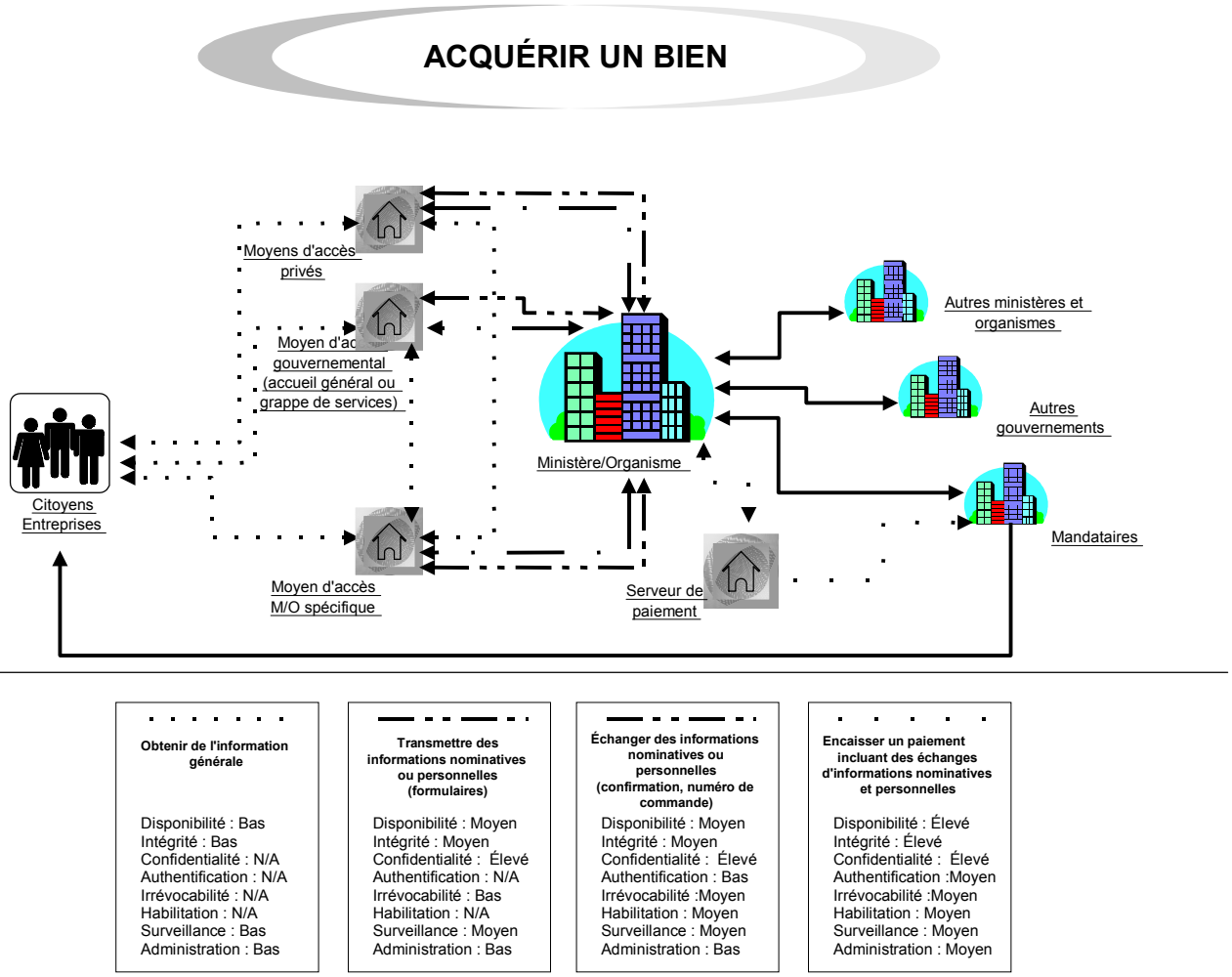
Échanger des informations nominatives ou personnelles (validation, piéces preuves, ...)

Disponibilité : Moyen
Intégrité : Moyen
Confidentialité : Élevé
Authentification : Élevé
Irrévocabilité :Moyen
Habilitation : Moyen
Surveillance : Moyen
Administration : Bas

Paiement de la prestation incluant des échanges d'informations nominatives et personnelles

Disponibilité : Élevé
Intégrité : Élevé
Confidentialité : Élevé
Authentification :Moyen
Irrévocabilité :Moyen
Habilitation : Moyen
Surveillance : Moyen
Administration : Moyen

6.3 Acquérir un bien



7. PRINCIPAUX IMPACTS RELATIFS À LA MISE EN ŒUVRE DE L'AGSIN

L'AGSIN propose une nouvelle vision de la sécurité de l'information numérique au sein de l'appareil gouvernemental québécois. De ce fait, elle engendre des nouveaux paradigmes en matière de sécurité qui découlent principalement des nouvelles possibilités d'affaires et des nouveaux canaux de distribution que sont les réseaux ouverts. Cette section présente les principaux impacts relatifs à la mise en œuvre de l'AGSIN. Ceux-ci serviront d'intrants au document « Recommandations de mise en œuvre ».

7.1 Le cadre de gouvernance

Il est essentiel que le gouvernement du Québec intègre l'AGSIN dans son modèle de gouvernance de la sécurité et dans le cadre de gestion des TI et de la PES sans lesquels elle ne peut tenir la route. Une très grande importance devra être apportée au cadre de gouvernance afin que les architectes qui utiliseront l'AGSIN dans le processus d'élaboration d'architecture de sécurité numérique au gouvernement du Québec puissent connaître leur contexte de travail.

La liste suivante énonce les principaux éléments à considérer qui devront être adressés dans le cadre de gouvernance :

- Général :
  - Responsable de l'AGSIN;
  - Application de l'AGSIN;
  - Suivi de l'AGSIN;
  - Évolution de l'AGSIN;
  - Communication de l'AGSIN.
- Reconnaissance des domaines de confiance :
  - Préparation d'un guide d'élaboration d'une politique de sécurité;
  - Préparation d'un guide d'élaboration d'un cadre de gestion de la sécurité.
- Reconnaissance des concepts :
  - Préparation d'un guide d'élaboration d'une entente;
  - Préparation d'un guide d'élaboration d'une interface sécuritaire.
- Détermination et vérification de l'utilisation des composantes;
  - Communes;
  - Partagés;
  - Réutilisables.
- Gestion du consentement :
  - Intégration les nouveaux principes généraux et spécifiques à la directive de sécurité;
  - Collaboration des responsables de la loi sur la protection des renseignements personnels.

7.2 La mise en commun et le partage

La mise en commun et le partage d'informations relatives à la sécurité nécessitent des infrastructures technologiques robustes. Les domaines de confiances responsables des informations identifiées comme ayant un potentiel de mise en commun ou de partage doivent s'assurer que celles-ci sont :

- Hautement disponibles (fréquemment sollicités);
- Rapidement accessibles (temps réponse);
- Facilement localisables;
- Protégées par des fonctions de sécurité adéquates.

La mise en commun et le partage d'applications relatives à la gestion de la sécurité et de modules de sécurité requiert que chaque domaine de confiance responsable de ces derniers mette en place une politique de sécurité et un cadre de gestion de la sécurité afin d'assurer une gestion adéquate de la base d'information en matière de sécurité et l'intégration des modules de sécurité aux applications d'entreprises.

La mise en commun et le partage d'infrastructures technologiques demandent que chaque domaine de confiance responsable porte une attention particulière aux infrastructures technologiques notamment au niveau de l'installation, de la paramétrisation et de la sécurisation du matériel (serveurs et équipements), des systèmes d'exploitation ainsi que des applications relatives à la gestion de la sécurité et/ou des modules de sécurité qui s'exécuteront sur ceux-ci.

Certaines études sont nécessaires afin de valider les potentiels de mise en commun et de partage identifiés dans les différentes vues du modèle général de l'AGSIN. Outre les informations, applications et infrastructures communes des répertoires gouvernementaux et certificats associés pour les employé(e)s et les partenaires/mandataires, qui font déjà l'objet d'études avancées, les potentiels de mise en commun et de partage identifiés doivent faire l'objet d'études particulières. Ces études particulières seront identifiées et adressées dans le plan de mise en oeuvre de l'AGSIN.

La section 4 couvre plus particulièrement le positionnement, la sécurité particulière et la concordance avec l'AGSIN de l'ICPG, du répertoire gouvernemental, de GIRES et du RICIB et du RETEM.

7.3 Les autres impacts

La gestion des informations de la base d'information en matière de sécurité de chaque domaine de confiance nécessite une connaissance approfondie des différents dépôts d'informations constituant cette base ainsi que des applications relatives à la gestion de la sécurité. Chaque domaine de confiance doit, dans la mesure de possible, effectuer une gestion centralisée de la base d'information en matière de sécurité répartie afin d'assurer une gestion complète de ces informations.

La mise en place des meilleures applications relatives à la gestion de la sécurité, modules de sécurité et infrastructures technologiques les supportant n'est pas garant de la sécurité si l'installation, la paramétrisation, la sécurisation et l'utilisation de ceux-ci sont effectuées de manière inadéquate. Des connaissances élargies des vulnérabilités et des façons d'y remédier au niveau matériel, logiciel et réseau sont également des éléments clés afin d'assurer le niveau de protection prévu. Chaque domaine de confiance doit élaborer une stratégie d'acquisition d'expertise (formation, embauche, services conseils, etc.) sur les produits sélectionnés et/ou développés afin d'assurer une gestion adéquate des applications

relatives à la gestion de la sécurité et à l'intégration des modules de sécurité aux applications d'entreprise et des infrastructures technologiques.

Des fonctions de sécurité, mécanismes de sécurité et solutions technologiques équivalents pour chaque mode d'accès retenus par les domaines de confiance doivent être disponibles afin d'assurer une gestion cohérente de la sécurité et favoriser une adhésion rapide des clientèles aux nouveaux modes d'accès électroniques aux services.

Plusieurs impacts potentiels en matière de sécurité spécifiques aux M/O ont été identifiés lors de l'état de la situation des ministères et organismes en matière de sécurité établie en date du 23 février 2001. Ces impacts devront, au besoin, être adressés par les domaines de confiance. Ces impacts, regroupés selon les dimensions de la sécurité, incluent :

- Juridique :
  - Modification des lois et règlements;
  - Modification aux contrats;
  - Analyses et avis juridiques;
  - Changement de culture (intégration papier/électronique).
- Humain et organisationnel :
  - Adaptation/élaboration du cadre de gestion de la sécurité (incluant normes, pratiques, mécanismes de contrôle);
  - Adaptation/élaboration des politiques et directives internes (incluant orientations et principes);
  - Adaptation/élaboration des processus et guides d'opérations;
  - Formation et sensibilisation du personnel;
  - Adaptation du service à la clientèle;
  - Intégration de la PES;
  - Gestion du changement;
  - Élaboration du plan de sécurité et du plan de communication;
  - Relations de travail;
  - Adaptation/élaboration des processus d'affaires;
  - Nouveaux rôles et/ou responsabilités en sécurité.
- Technologique :
  - Adaptation/élaboration du cadre de développement et d'acquisition;
  - Ajout de nouvelles fonctions de sécurité;
  - Mise à jour des technologies et ajout de nouvelles technologies;
  - Adaptation/élaboration de l'architecture technologique et de sécurité.

Annexe A

Références

Documents du gouvernement québécois:

Architecture gouvernementale de la sécurité de l'information numérique – Portrait et besoins gouvernementaux (bien livrable 1), Secrétariat du Conseil du trésor, mai 2001

Architecture gouvernementale de la sécurité de l'information numérique – Orientations et principes (bien livrable 2), Secrétariat du Conseil du trésor, avril 2001

XML en route au gouvernement du Québec : Rapport de recherche-consultation réalisée pour le Secrétariat du Conseil du trésor du Québec, Groupe départemental de Recherche sur les Documents Structurés, École de Bibliothéconomie et des Sciences de l'Information, Université de Montréal, février 2001

Modèle de gestion de la sécurité des systèmes d'information dans l'administration québécoise, Secrétariat du Conseil du trésor, février 2001

Architecture technologique du projet GIRES, Secrétariat du Conseil du trésor, mars 2000

Guide relatif à la catégorisation de l'information numérique et aux mesures généralement appliquées en matière de sécurité, Conseil du trésor du Québec, 2000

Architecture d'entreprise gouvernementale (AEG) – Contexte, perspectives et architecture de haut niveau, Document de travail, Conseil du trésor du Québec, 2000

Fiches de rencontres menées dans le cadre des travaux de l'AEG, février 2000

Infrastructure à clés publiques gouvernementale, Conseil du trésor du Québec, 2000

Recueil des pratiques recommandées en matière de sécurité de l'information numérique, Secrétariat du Conseil du trésor, décembre 1999

Solution GIRES, Sommaire exécutif

Directive sur la sécurité de l'information et des échanges électroniques dans l'Administration gouvernementale, Conseil du trésor du Québec, septembre 1999

La politique québécoise de l'autoroute de l'information – Agir autrement, Conseil du trésor du Québec, 1998

Sécurité des échanges électroniques au gouvernement du Québec , Conseil du trésor du Québec,1997

Conception détaillée du répertoire gouvernemental québécois, Sous-secrétariat à l'inforoute et aux ressources informationnelles, Secrétariat du Conseil du trésor, décembre 1997

Présentation *Sertir, Serveur transactionnel d'information et de repérage*, Services gouvernementaux du Conseil du trésor

Le droit d'auteur au Canada – Bases , Publications du Québec, http://publicationsduquebec.gouv.qc.ca/fr/droitauteur/html/droit_auteur_gen.dbml

Documents de gouvernements étrangers :

Richard A. Guida, *Memorendum to File: Report of Trip to London, England to Attend Meeting Among Governments of the U.K., Canada, and Australia (Plus Related Ancillary Meetings)*, Federal Public Key Infrastructure Steering Committee, 30 novembre 2000

Information Age Government : Benchmarking Electronic Service Delivery, Central IT Unit, juillet 2000

The Evolving Federal Public Key Infrastructure, Federal Public Key Infrastructure Steering Committee & Federal Chief Information Officiers Council, juin 2000

Statewide Technical Architecture Document - Chapter 12 : Security and Directory Service Architecture, State of North Carolina, mai 2000

Sécurité de l'information : Accroître la sécurité de l'information, Rapport à l'intention du Conseil des DPI du secteur public [canadien], version 1.0, Sous-comité sur la protection de l'information, 14 avril 2000

Orientations pour l'architecture IDA, Commission européenne DG III/B/6, mars 1999

Manuel canadien de la sécurité des technologies de l'information - MG9, gouvernement du Canada, Centre de la sécurité des télécommunications, mars 1998

Norme de sécurité technique dans le domaine de la technologie de l'information, Gendarmerie royale du Canada, août 1997

Textes légaux

Québec :

Loi sur les archives, L.R.Q., 1983, c. A-21.1

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, L.R.Q., 1982, c. A-2.1

Loi sur l'administration publique, L.Q., 2000, c. 8

Loi concernant le cadre juridique des technologies de l'information, P.L.Q. 161, 2001, c. 32

Code civil du Québec, L.Q., 1991, c. 64

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., 1993, c. P-39.1

Charte des droits et libertés de la personne, L.R.Q., c. C-12

Canada :

Loi sur la protection des renseignements personnels et les documents électroniques (C-6), L.C., 2000, c. 5

Loi sur le droit d'auteur, L.R.C., 1985, c. C-42

Charte canadienne des droits et libertés, annexe B de la Loi de 1982 sur le Canada, 1982, c. 11

Loi sur les marques de commerce, L.R.C, 1985, c. T-13

Autres documents :

AGSIN : Commentaires sur le troisième bien livrable produit par CGI et daté du 24 avril 2001, Gartner Consulting, 2 mai 2001

La réalité des travaux d'architecture, Gartner Group, 2001

Warwick Ford et Michael S. Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption*, Prentice Hall PTR, 2001

Michele D. Guel, *SANS Network Security Roadmap 2001, 4e édition*, SANS Institute, hiver 2001

Dutrisac, Robert, *La CAI dit non au projet de carte santé*, Le Devoir, 20 février 2001

W. Malik, *Do Security Products Alone Solve the Problem?*, Gartner Group, 16 janvier 2001

Ant Allan, *Security Applications of Smart Cards: Perspective*, Gartner Group, 10 janvier 2001

Steve Hunt et Jan Sundgren, *Security Trends for 2001: Extranets Turn Up the Heat*, Giga Information Group, 2 janvier 2001

Key Trends for 2001: Mobile Devices, Giga Information Group, IdeaByte, , 29 novembre 2000

Chris Christiansen, Nora S. Freedman, Brian Burke et Charles Kolodgy, *1999 Token and IT Authentication Market*, IDC, novembre 2000

Christian A. Christiansen, Charles Kolodgy, Brian Burke et Nora Freedman, *Biometrics Market and Forecast: The Future of Hardware Authentication?*, novembre 2000

V. Wheatman, *Resolving the Unresolved Issues in PKI*, Gartner Group, 16 octobre 2000

Steve Hunt, *Securing the Extranet Web Application*, Giga Information Group, 5 septembre 2000

Jonathan Penn, *The Marginalizing of X.500*, Giga Information Group, 30 août 2000

Christian A. Christiansen, Brian E. Burke et Nora Freedman, *Internet Security Software Market Forecast and Analysis, 2000–2004*, IDC, avril 2000

Jim Slaby, *The Current State of Enterprise Internet VPN Technology*, Giga Information Group, 25 février 2000

Vic Wheatman, *The Role of Smart Cards in PKI*, Gartner Group, 17 septembre 1999

Critères communs pour l'évaluation de la sécurité des TI (Critères communs), version 2.1 (3 parties), Common Criteria Organization, août 1999. Version 2.0 disponible en français à http://www.cse-cst.gc.ca/cse/criteria/francais/publicat.htm#Common_Criteria

Méthodologie commune pour l'évaluation de la sécurité des TI, version 1.0 (2 parties), Common Criteria Organization, août 1999. Disponible en anglais à : http://209.116.65.120/docs/index.html. Version 0.6 disponible en français à http://www.cse-cst.gc.ca/cse/criteria/francais/publicat.htm#Common_Criteria

Generally Accepted System Security Principles - version 2.0, International Information Security Foundation (I^2SF), juin 1999

Andrew Bartels, *The Whys and Means of Online Authentication*, Giga Information Group, 9 février 1999

Charles Cresson Wood, *Best Practices in Internet Commerce Security*, CommerceNet Research Report, 1ier août 1998

Public Key Infrastructure Overview – Attribute Certificates, Baltimore Technologies, http://www.baltimore.com/devzone/pki/attributecertificates.html

Annexe B

Glossaire

Généralités :

Besoin d'affaires : Exigences nées d'une série de processus, ayant chacun une finalité clairement définie, impliquant plus d'une organisation, réalisés par échange d'informations et tendant à l'accomplissement d'un objectif accepté par accord mutuel pour une certaine période de temps.[Définition inspirée de la norme ISO/IEC 14662].

Domaine de confiance : Un ensemble d'éléments d'ordre juridique, humain, organisationnel et technologique, un cadre de gestion de la sécurité et un ensemble d'activités pertinentes à la sécurité qui sont tous assujettis à une politique de sécurité administrée par une seule autorité en matière de sécurité. [Définition inspirée de la norme ISO/IEC 10181-1].

Entente : Définit les règles qui régissent les interactions entre les domaines de confiance ainsi qu'avec les clientèles. Elle permet également de délimiter les champs de compétence entre les domaines de confiance. Une Entente contient au minimum une Interface sécuritaire. [Définition inspirée de la norme ISO/IEC 10181-1].

Fonction de sécurité : Fonction, fournie par une couche de systèmes ouverts, garantissant une sécurité des systèmes et du transfert de données. [Définition inspirée de la norme ISO 7498-2].

Interface sécuritaire : Définit les modalités techniques de sécurisation de l'information numérique. Elle est un ensemble d'éléments, comprenant à la fois des aspects logiciels et matériels, qui présente les normes et les fonctions de sécurité nécessaires pour assurer la connectivité et l'interopérabilité entre les domaines de confiance ainsi qu'avec les clientèles. [Définition inspirée de Orientations pour l'architecture IDA, Commission européenne, mars 1999].

Mécanisme de sécurité : Les mécanismes de sécurité sont des processus, logiciels ou équipements technologiques ayant pour but de remplir les diverses fonctions de sécurité.

Norme de jure (ou «norme») : Norme définie et adoptée par un organisme officiel de normalisation, sur le plan national ou international. À noter que « De jure » (« from the law » ou « de droit ») s'oppose à « de facto » (« from the fact » ou « de fait »). Il est parfois conseillé de réserver le terme « norme » à celle qui est reconnue par un organisme officiel et « standard » à celle qui ne l'est pas, mais qui s'est imposée de soi.[Grand dictionnaire terminologique, Office de la langue française, 2000]

Norme de facto (ou «standard») : Norme qui n'a pas été définie ni entérinée par un organisme officiel de normalisation comme l'ISO, l'AFNOR, l'IETF, etc., mais qui s'est imposée par la force des choses, parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'entreprises ou encore d'un consortium. Une norme de facto peut découler des spécifications décrites par une seule entreprise (en anglais, « proprietary standard »). À noter qu'on parle aussi, mais plus rarement, de « quasi-standard » pour désigner une norme de facto. Aujourd'hui, en informatique, il n'est pas rare qu'une norme de facto devienne une norme de jure.[Grand dictionnaire terminologique, Office de la langue française, 2000]

Règle architecturale : Vise à définir à un niveau de détails plus précis, les règles applicables à chacune des fonctions de sécurité. Elle oriente la conduite des travaux et porte sur les éléments à considérer lors de l'élaboration d'une architecture détaillée de sécurité.

Solutions technologiques : Les solutions technologiques sont des ensembles de solutions permettant la gestion des différents mécanismes de sécurité.

Transaction d'affaires : Ensemble prédéterminé d'activités menées par des organisations et/ou de procédures qu'elles suivent qui vise à atteindre dans les affaires un but expressément partagé, terminé lorsqu'est observée une des conclusions convenues par toutes les organisations prenantes, bien que cette observation puisse être partiellement implicite.[ISO/IEC 14662]

Mécanismes et solutions technologiques :

Analyseur de vulnérabilités : Outil permettant de tester la robustesse des infrastructures technologiques et des applications de sécurité. Les analyseurs de vulnérabilités sont basés sur deux approches, soit l'analyse des vulnérabilités basée sur les réseaux et celle basée sur les serveurs. Le premier type permet de simuler le comportement d'attaquants afin de mettre en évidence les faiblesses des systèmes qui sont testés alors que le deuxième type vérifie les paramétrisations des systèmes de façon à déterminer si elles sont consistantes avec les politiques de sécurité de l'organisation. Thresher de farm9.com, Internet Scanner de ISS, by-Control for Internet Security de BindView, System Scanner et Database Scanner de ISS, SecurityAnalyst de Intrusion.com et VigilEnt Security Agents de PentaSafe sont quelques-uns des produits de ce type disponibles sur le marché. [Définition inspirée de Roadmap To Security Tools & Services, SANS Institute, 4e édition, hiver 2001].

Balancement des charges : Fonctionnalité assurée par des logiciels ou équipements permettant de répartir efficacement la charge à travers plusieurs serveurs ou applications lorsque ceux-ci sont très sollicités. [Définition propre à l'AGSIN].

Biométrie : Analyse mathématique des caractéristiques biologiques d'une personne, destinée à déterminer son identité de manière irréfutable. Les caractéristiques biométriques utilisées pour l'authentification sont les empreintes digitales, les données sur l'iris, la géométrie de la main et du visage, la signature, l'empreinte vocale et l'ADN. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000].

Carte à puce : Carte en plastique, d'un format généralement normalisé, dotée de microcircuits pouvant contenir une simple mémoire ou un microprocesseur programmable. La carte à puce couplée à un mot de passe forme le processus d'authentification. L'utilisateur doit d'abord entrer son mot de passe, puis insérer la carte pour avoir accès à son contenu. Ce contenu peut consister en un certificat ou en informations diverses. Une variante consiste en un jeton qui se branche dans le port USB. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000].

Certificat d'attributs : Une structure similaire à un certificat de clé publique qui ne contient pas de clé publique mais plutôt des attributs qui spécifient l'appartenance à un groupe, les rôles, les privilèges de sécurité ou toutes autres informations d'habilitation associées au détenteur du certificat d'attribut. [Public Key Infrastructure – Attribute Certificates, Baltimore Technologies].

Certificat de clé publique de chiffrement : Document électronique délivré par une autorité de certification (une constituante d'une ICP), qui garantit l'authenticité d'une clé publique de chiffrement. [Grand dictionnaire terminologique, Office de la langue française, 2000].

Certificat de clé publique de signature : Document électronique délivré par une autorité de certification (une constituante d'une ICP), qui garantit l'authenticité d'une clé publique de signature. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000].

Chiffrement des données : Transformation de données par cryptographie au niveau des données et des applications. [Définition inspirée de Orientations pour l'architecture IDA, Commission européenne, mars 1999].

Chiffrement des communications : Transformation de données par cryptographie au niveau des communications. [Définition inspirée de Orientations pour l'architecture IDA, Commission européenne, mars 1999].

Code d'authentification de message (CAM) : Sceau électronique produit par un algorithme à clé secrète et permettant de garantir l'intégrité d'un message à l'arrivée. [Grand dictionnaire terminologique, Office de la langue française, 2000].

Code d'usager : Identifiant prenant la forme d'un code alphanumérique unique, qui est attribué à un utilisateur pour le distinguer des autres utilisateurs d'un système informatique. [Grand dictionnaire terminologique, Office de la langue française, 2000]

Console de surveillance unifiée : Système permettant aux gestionnaires de sécurité de gérer diverses solutions de sécurité en temps presque réel à travers une console de gestion unifiée. Ces solutions simplifient ainsi la gestion de la sécurité et permettent de réassigner le personnel dont la tâche consiste à surveiller et à gérer les divers produits de sécurité. À titre d'exemples de produits de ce type, notons entre-autres Open e-Security Platform de e-Security, Harvester de form9.com, ISS Emergency Response Services de ISS et by-Control de BindView. [Définition inspirée de Roadmap To Security Tools & Services, SANS Institute, 4e édition, hiver 2001]

Coupe-feu : Application ou équipement qui contrôle les accès à un réseau et surveille le flot du trafic sur le réseau. Un coupe-feu peut filtrer et éloigner le trafic qui n'est pas voulu et éviter les intrusions dans un réseau privé. [Définition propre à l'AGSIN].

Empreinte numérique (ou condensé) : Condensé numérique, identifié par une séquence de caractères, qui représente le contenu d'un message, sans le révéler, dont la valeur unique est produite par un algorithme de hachage, et qu'on utilise pour créer une signature numérique, afin d'authentifier le message ou de vérifier l'identité de son auteur. [Grand dictionnaire terminologique, Office de la langue française, 2000]

Infrastructure à clés publiques (ICP) : Système permettant la gestion de clés de chiffrement et la délivrance de certificats numériques. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000]

Infrastructures de gestion des privilèges : Outils commerciaux ayant pour but d'intégrer dans une seule application la gestion de l'authentification et de l'habilitation de multiples plate-formes et applications. Ces outils permettent entre autres : le support de multiples méthodes d'identification/authentification, la gestion par politiques ou règles, la gestion à l'aide de technologies de répertoire ou par base de données, l'ouverture de session simplifiée, la délégation de la sécurité à des niveaux inférieurs, etc. À titre d'exemples de produits de ce type, notons entre-autres GetAccess de Entrust, SiteMinder de Netegrity, NetPoint de Oblix, ClearTrust SecureControl de Securant et Tivoli SecureWay d'IBM sont des exemples de ce type de produits. [Définition propre à l'AGSIN]

Interface de programmation d'applications (API) : Ensemble de sous-routines ou de fonctions qu'un programme ou une application peut appeler pour indiquer au système d'exploitation d'effectuer une tâche spécifique. [Orientations pour l'architecture IDA, 3e partie, Commission européenne, mars 1999]

Jeton : Dispositif que l'on transporte avec soi ou et qui sert à produire des codes ou des mots de passe à partir desquels l'appareil qui les reçoit peut reconnaître l'identité de la personne qui désire obtenir l'accès à un réseau, à un système ou à un ordinateur. Permet l'authentification moyenne à forte. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000]

Journalisation des accès : Méthode d'enregistrement, de traitement et d'examen des journaux d'accès pour y rechercher des événements clés ou résumés. [Orientations pour l'architecture IDA, Commission européenne, mars 1999]

Mécanismes d'habilitation des applications : Mécanismes d'habilitation et de contrôle d'accès de base inclus dans les applications d'entreprises. [Définition propre à l'AGSIN]

Mécanismes d'habilitation des systèmes d'exploitation (NOS/OS) : Mécanismes d'habilitation et de contrôle d'accès de base inclus dans les systèmes d'exploitation. [Définition propre à l'AGSIN]

Mécanismes d'habilitation des SGDB : Mécanismes d'habilitation et de contrôle d'accès de base inclus dans les systèmes de gestion de bases de données. [Définition propre à l'AGSIN]

Moniteur de contenu actif : Outil qui examine le contenu pénétrant dans un ordinateur ou un réseau à la recherche de contenu pouvant potentiellement faire des dommages (virus, Java et Active-X malicieux, etc.) en comparant ce contenu à des définitions incluses dans des librairies de définitions continuellement mises à jour. SuperScout de SurfControl, SurfinGate de Finjan Software et ConsoleServer 3200 de Lightwave Communications sont des exemples de ce type de produits. [Définition inspirée de Roadmap To Security Tools & Services, SANS Institute, 4e édition, hiver 2001]

Mot de passe : Authentifiant prenant la forme d'une chaîne de caractères, d'un code secret choisi par l'utilisateur, que celui-ci doit entrer lors de la procédure d'accès à un système. La connaissance du mot de passe associé à l'identification de l'utilisateur est considérée comme une preuve d'autorisation d'accès. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000]

Notarisation : Enregistrement des éléments essentiels d'une transaction entre deux parties chez un tiers de confiance, lequel peut ultérieurement en garantir l'exactitude. [Grand dictionnaire terminologique, Office de la langue française, 2000]

Numéro d'identification personnelle : Authentifiant prenant la forme d'un code numérique, qui est attribué à un utilisateur, lui permettant ainsi d'obtenir l'accès à un système et d'y effectuer l'opération désirée. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000]

Outils d'audit : Outils, généralement inclus avec les systèmes d'exploitation ou du domaine public, qui permettent de déceler des vulnérabilités précises telles que les CGI vulnérables, les mots de passe facilement détectables, les structures de bases de données fragiles, etc. Ces outils spécialisés peuvent dans certains cas être remplacés par des outils plus polyvalents tels que les détecteurs d'intrusions, les analyseurs de vulnérabilités, etc. [Définition propre à l'AGSIN].

Outils d'ouverture de session : Outils permettant la gestion centralisée et simplifiée des ouvertures de session. [Définition propre à l'AGSIN].

Outils de consolidation des journaux : Outils permettant la consolidation et l'analyse automatisée des journaux. [Définition propre à l'AGSIN].

Redondance : Duplication d'un élément essentiel au fonctionnement normal du système informatique (données, applications, infrastructures technologiques, etc.) en vue de pallier la défaillance éventuelle de cet élément et d'assurer ainsi la continuité d'une activité vitale. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000].

Relève : Processus et outils permettant la reprise d'une production informatique détériorée ou détruite par un sinistre matériel ou immatériel, que celui-ci soit partiel ou total. [Grand dictionnaire terminologique, Office de la langue française, 2000].

Répertoire : Mécanisme d'entreposage pour des noms et adresses d'entités (personnes, applications) devant être associées à des certificats de clé publique afin de garantir leur identification et leurs autorisations dans le fonctionnement normal et en sécurité des affaires. Un répertoire peut aussi contenir des certificats d'attributs permettant l'habilitation des entités. [Définition propre à l'AGSIN]

Sauvegarde : Processus et outils ayant pour but de recopier un ou plusieurs fichiers de données, généralement sur un support externe, afin d'en prévenir la perte systématique ou accidentelle. [Définition inspirée du Grand dictionnaire terminologique, Office de la langue française, 2000].

Système de détection des intrusions : Les détecteurs d'intrusions sont basés principalement sur deux approches, soit la détection des intrusions sur les réseaux et la détection des intrusions sur les serveurs. Un système de détection d'intrusion sur les réseaux surveille le trafic sur les réseaux et émet une alarme lorsqu'il identifie un « pattern » de trafic qu'il perçoit être une tentative de balayage, un refus de service ou une autre attaque. Un système de détection d'intrusion sur les serveurs est un logiciel qui surveille les fichiers de journalisation des systèmes et applications qui émet une alarme lorsqu'un utilisateur essai d'atteindre des données, fichiers ou services non autorisés. Real Secure de ISS, NetProwler et Intruder Alert de Symantec, SecureNetPro de Intrusion.com, Entercept de Entercept Security et PentaSafe VigilEnt Security Agents de PentaSafe sont des exemples de ce type de produits. [Définition inspirée de Roadmap To Security Tools & Services, SANS Institute, 4^{e} édition, hiver 2001].

Système de détection des virus : Logiciel de sécurité qui procède, automatiquement ou sur demande, à l'analyse des fichiers et de la mémoire des ordinateurs, soit pour empêcher toute introduction parasite, soit pour détecter et éradiquer tout virus dans un système informatique. Norton Antivirus de Symantec, InoculateIT de Computer Associates et VirusScan, WebShield, NetShield et GroupShield de Network Associates sont des exemples de ce type de produits. [Grand dictionnaire terminologique, Office de la langue française, 2000].

Système de surveillance des réseaux, serveurs et stations : Outil permettant la paramétrisation, l'administration, le monitorage et la correction des problèmes de réseaux, serveurs et équipements de communication. CiscoWorks de Cisco, Unified Network Management de Nortel, Tivoli de IBM, Unicenter TNG de Computer Associates et Reporting Module de Check Point sont des exemples de cette catégorie de produits. [Définition propre à l'AGSIN].

Technologies de grappes (« clustering ») : Technologies permettant de connecter deux ou plusieurs serveurs (logiciels ou équipements) de façon à ce que ceux-ci se comportent comme un seul serveur. Ces technologies sont utilisées pour garantir le traîtement parallèle, le balancement des charges et la tolérance aux pannes. [Définition inspirée de www.webopedia.com].

Annexe C

Résultats des cueillettes auprès des M/O

Cueillette sur la prestation électronique de services (PES) protégés

	MO1		MO2		MO3		MO4		MO5		MO6		MO7		MO8		MO9		M10		Total	
	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non	Oui	Non
Est-ce que votre M/O s'est engagé dans un processus de PES ?	1		1		1		1		1		1		1		1		1		1		10	0
Est-ce que des liens avec d'autres M/O, des partenaires ou des mandataires sont envisagés pour une ou plusieurs PES ?	1		1		1		1		1		1		1		1		1		1		10	0
Est-ce l'information à l'intérieur d'une ou plusieurs PES a été classifiée ?	1			1	1					1	1		1		1		1		1		7	2
Est-ce qu'une analyse de vulnérabilité a été conduite pour la ou les PES ?	1		1		1		1			1	1		1		1		1			1	8	2
Est-ce que le cadre de gestion de la sécurité de votre M/O est adapté aux PES ?	1	1		1	1		1			1	1			1	1		1			1	6	5
Est-ce que le cadre juridique général et spécifique de votre M/O est adapté aux PES?	1	1		1		1	1			1		1	1	1	1			1		1	4	8
Avez-vous une architecture de sécurité ? Si oui, est-ce que l'architecture de sécurité de votre M/O est adaptée aux PES?	1		1		1		1			1	1		1		1		1			1	8	2
Est-ce que votre M/O utilise ou envisage d'utiliser des infrastructures communes gouvernementales de sécurité (ex: services de certification; etc.) ?		1		1	1		1			1	1		1		1		1		1		7	3

Cueillette sur la prestation électronique de service (PES) protégées

Stade d'avancement ?	AF	C	MO	EX
MO1	1	1	1	1
MO2			1	
MO3				1
MO4			1	
MO5	1			
MO6				1
MO7	1			
MO8	1	1	1	
MO9	1	1	1	1
MO10	1			
Total	6	3	5	4

AF: analyse de faisabilité C: conception MO: mise en œuvre EX: Exploitation

Quelle est la clientèle visée par la /les PES de votre	C	E	M	P	M/O
MO1	1			1	1
MO2	1	1			
MO3	1				1
MO4	1	1			
MO5					1
MO6	1	1	1	1	1
MO7	1		1	1	
MO8	1	1	1		
MO9	1	1			
MO10			1	1	
Total	8	5	4	4	4

C: Citoyen E: Entreprise M: Mandataire P: Partenaire M/O: Ministère et organisme

Section sur les dimensions et les domaines de la sécurité

Quels sont les éléments de la dimension juridique (cadre de sécurité légal) que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 1**			**M/O 2**			**M/O 3**			**M/O 4**			**M/O 5**			**M/O 6**			**M/O 7**		
	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Convention internationale	1					1		1				1	1					1			1
Lois nationales (Canada)	1					1	1					1			1	1			1		
Lois nationales (hors Canada)			1			1		1				1			1			1			1
Lois provinciales (hors Québec)			1			1	1					1	1			1			1		
Lois provinciales générales (Québec)	1			1			1			1			1			1			1		
Lois provinciales spécifiques (Québec)	1			1			1			1			1			1			1		
Règlements généraux	1			1			1					1	1					1	1		
Règlements spécifiques	1					1	1			1			1					1	1		
Avis juridiques	1					1	1			1			1					1	1		
Élaboration de contrats	1			1			1			1			1					1	1		
Autres										1											
Quels sont les éléments de la dimension organisationnelle (cadre de gestion de la sécurité) que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 1**			**M/O 2**			**M/O 3**			**M/O 4**			**M/O 5**			**M/O 6**			**M/O 7**		
Dans le domaine de la sécurité administrative et organisationnelle	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Classification de l'information		1		1				1			1		1	1			1		1		
Analyse de risques et de vulnérabilités	1			1			1			1			1			1			1		
Politique de sécurité	1			1			1			1			1			1			1		
Directive de sécurité	1				1		1					1	1			1			1		
Normes et pratiques de sécurité	1			1			1			1			1			1			1		
Identification d'un RSIN	1			1			1			1			1			1			1		
Guide et procédures de sécurité	1			1			1			1			1			1			1		
Registre d'autorités de sécurité (détenteurs)	1			1	1		1			1			1			1			1		
Registre des utilisateurs ou groupes d'utilisateurs	1			1			1			1			1					1	1		
Registre du matériel	1			1			1			1			1			1			1		
Registre des logiciels	1			1					1	1			1			1			1		
Registre des fichiers ou des données ou des systèmes	1			1					1	1			1			1			1		
Plan global de sécurité	1			1					1	1			1	1			1		1		
Mécanismes de contrôle et de suivi ainsi que proccessus d'audit	1			1					1	1			1			1			1		
Dans le domaine de la sécurité relié au personnel	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Enquête de sécurité	1			1					1			1	1				1				1
Habilitation sécuritaire (ex: processus d'accréditation)	1				1				1			1			1			1			1
Plan de sensibilisation	1			1					1	1			1				1		1		
Plan de formation	1				1				1	1			1				1		1		
Dans le domaine de la sécurité des opérations	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Gestion des accès aux systèmes et des autorisations	1			1					1	1			1			1			1		
Procédures et contrôles	1			1					1	1			1				1		1		
Supports	1			1					1	1			1					1	1		
Plan et mesures d'urgence	1			1					1	1			1	1		1			1		
Plan de relève et continuité	1			1	1				1	1			1			1			1		
Autres									1	1									1		
Domaine de la sécurité physique et du milieu	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Installations principales et auxiliaires des ressources infomationnelles	1			1			1			1			1			1			1		
Contrôle de l'accès physique	1			1			1			1			1			1				1	
Rangement des supports d'informations numériques et des ressources infomationnelles			1	1			1			1			1			1			1		
Destruction des supports d'informations numériques et des ressources infomationnelles	1			1			1			1			1			1			1		
Envoi et transport des supports d'informations numériques et des ressources infomationnelles	1			1			1			1			1			1			1		
Protection contre les désastres et les incendies	1			1			1			1			1			1			1		

Section sur les dimensions et les domaines de la sécurité

Quels sont les éléments de la dimension juridique (cadre de sécurité légal) que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 8**			**M/O 9**			**M/O 10**			**M/O 11**			**M/O 12**			**Total**		
	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Convention internationale			1			1	1					1		1		3	2	7
Lois nationales (Canada)	1					1	1					1			1	6	0	6
Lois nationales (hors Canada)			1			1			1			1			1	0	1	11
Lois provinciales (hors Québec)			1			1			1			1			1	4	0	8
Lois provinciales générales (Québec)	1			1			1			1			1	1		12	1	0
Lois provinciales spécifiques (Québec)	1			1			1			1			1			12	0	0
Règlements généraux	1			1			1					1			1	8	0	4
Règlements spécifiques			1	1			1			1					1	8	0	4
Avis juridiques	1			1			1			1					1	9	0	3
Élaboration de contrats			1	1			1			1			1			10	0	2
Autres																1	0	0
Quels sont les éléments de la dimension organisationnelle (cadre de gestion de la sécurité) que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 8**			**M/O 9**			**M/O 10**			**M/O 11**			**M/O 12**			**Total**		
Dans le domaine de la sécurité administrative et organisationnelle	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Classification de l'information			1	1			1			1			1			7	5	1
Analyse de risques et de vulnérabilités	1			1			1	1		1			1			12	1	0
Politique de sécurité	1			1			1				1		1			11	1	0
Directive de sécurité	1			1			1			1			1			10	1	1
Normes et pratiques de sécurité	1			1			1			1			1			12	0	0
Identification d'un RSIN	1			1			1			1			1			12	0	0
Guide et procédures de sécurité		1		1			1			1				1		10	2	0
Registre d'autorités de sécurité (détenteurs)	1			1			1				1			1		10	3	0
Registre des utilisateurs ou groupes d'utilisateurs	1			1			1				1			1		9	2	1
Registre du matériel	1			1			1			1				1		11	1	0
Registre des logiciels	1			1			1			1				1		10	1	1
Registre des fichiers ou des données ou des systèmes	1			1			1			1				1		10	1	1
Plan global de sécurité		1		1			1			1			1			9	3	1
Mécanismes de contrôle et de suivi ainsi que proccessus d'audit		1		1			1	1			1			1		8	4	1
Dans le domaine de la sécurité relié au personnel	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Enquête de sécurité			1	1			1					1			1	5	1	6
Habilitation sécuritaire (ex: processus d'accréditation)			1	1					1			1		1		2	2	8
Plan de sensibilisation			1	1			1					1		1		7	2	3
Plan de formation			1	1			1					1		1		6	3	3
Dans le domaine de la sécurité des opérations	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Gestion des accès aux systèmes et des autorisations	1			1			1			1			1			11	0	1
Procédures et contrôles	1			1			1			1			1			10	1	1
Supports			1	1			1			1			1			9	0	3
Plan et mesures d'urgence	1			1			1			1				1		10	2	1
Plan de relève et continuité	1			1				1		1				1		9	3	1
Autres				1						1						4	0	1
Domaine de la sécurité physique et du milieu	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Installations principales et auxiliaires des ressources infomationnelles	1			1			1			1			1			12	0	0
Contrôle de l'accès physique	1			1			1			1			1			11	1	0
Rangement des supports d'informations numériques et des ressources infomationnelles			1	1			1			1			1			10	0	2
Destruction des supports d'informations numériques et des ressources infomationnelles			1	1			1			1			1			11	0	1
Envoi et transport des supports d'informations numériques et des ressources infomationnelles			1	1			1			1			1			11	0	1
Protection contre les désastres et les incendies			1	1			1			1			1			11	0	1

Quels sont les éléments de la dimension technologique (composantes physiques et solutions technologiques) que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 1**			**M/O 2**			**M/O 3**			**M/O 4**			**M/O 5**			**M/O 6**			**M/O 7**		
Domaine de la sécurité du matériel	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Dispositifs de sécurité	**1**			**1**			**1**			**1**			**1**			**1**			**1**		
Entretien et soutien du matériel	**1**			**1**			**1**			**1**			**1**					**1**	**1**		
Contrôle de la qualité	**1**			**1**				**1**		**1**			**1**			**1**			**1**		
Domaine de la sécurité des logiciels	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Normes de conception, élaboration, entretien, contrôle de la qualité et essais de réception	**1**			**1**			**1**			**1**			**1**			**1**			**1**		
Logiciels d'exploitation	**1**			**1**			**1**			**1**			**1**			**1**			**1**		
Gestion des données et de la base de données	**1**			**1**			**1**			**1**			**1**			**1**			**1**		
Logiciels d'application	**1**			**1**			**1**			**1**			**1**			**1**			**1**		
Domaine de la sécurité des communications	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Entretien et soutien des communications (infrastructures de télécommunications)	1			1			1			1			1			1			1		
Logiciels de communication	**1**			**1**			**1**			**1**			**1**			**1**			**1**		
Protection de l'information transmise sur un réseau de communication	**1**			**1**			**1**			**1**			**1**				**1**		**1**		

Section sur la prévention, la détection, la correction et l'assurance de la sécurité

Quels sont les éléments de prévention, de détection, de correction et d'assurance que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 1**			**M/O 2**			**M/O 3**			**M/O 4**			**M/O 5**			**M/O 6**			**M/O 7**		
	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Technologies de Coupe-feu ou de garde-barrière	1			1			1			1			1			1			1		
Technologies de réseau virtuel privé (RVP)			**1**	**1**			**1**				**1**			**1**				**1**	**1**		
Technologies de serveur de cache ou proxy	**1**			**1**				**1**		**1**			**1**			**1**			**1**		
Outils ou services d'analyse de vulnérabilités (réseau, serveur et donnée)	**1**				**1**			**1**		**1**			**1**				**1**		**1**		
Outils ou services de détection des intrusions (réseau, serveur et donnée)			**1**		**1**			**1**		**1**			**1**				**1**		**1**		
Outils ou services de protection des données et des programmes (poste et	**1**			**1**			**1**				**1**		**1**					**1**	**1**		
Outils ou services de surveillance (réseau, serveur, contenu, anti-virus)	**1**			**1**			**1**			**1**					**1**		**1**		**1**		
Outils ou services de journalisation et conciliation des journaux	**1**			**1**				**1**		**1**			**1**			**1**			**1**		
Outils ou services de gestion de la sécurité (centralisé, répartis, externe)	**1**			**1**				**1**		**1**			**1**					**1**	**1**		
Outils ou services de garantie de haute disponibilité (technologie de grappe, de partage de charge, de relève)	**1**			**1**				**1**			**1**				**1**	**1**				**1**	
Autres																					

Section sur l'utilisation d'outils et de services spécialisés favorisant DICAI

Quels sont les outils et services spécialisés que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 1**			**M/O 2**			**M/O 3**			**M/O 4**			**M/O 5**			**M/O 6**			**M/O 7**		
	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Outils ou services d'ICP	1			1				1			1		1					1		1	
Outils ou services de répertoire		**1**			**1**			**1**		**1**				**1**		**1**			**1**		
Outils ou services d'ouverture de session simplifiée (serveurs spécialisés, etc.)					**1**			**1**			**1**		**1**					**1**	**1**		
Outils ou services d'authentification (cartes à puces, jetons, serveurs spécialisés, etc.)		**1**		**1**				**1**		**1**	**1**		**1**					**1**	**1**		
Outils ou services de contrôle des accès (certificats d'attributs, jetons, serveurs spécialisés, etc.)		**1**		**1**				**1**		**1**	**1**		**1**				**1**		**1**		
Outils ou services de chiffrement (données et sessions)	**1**			**1**				**1**		**1**				**1**			**1**				**1**
Outils ou services de contrôle d'intégrité (serveurs, données et sessions)	**1**			**1**				**1**			**1**			**1**			**1**				**1**
Outil ou service de gestion du consentement		**1**			**1**			**1**			**1**			**1**				**1**			**1**
Autres																					

Quels sont les éléments de la dimension technologique (composantes physiques et solutions technologiques) que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 8**			**M/O 9**			**M/O 10**			**M/O 11**			**M/O 12**			**Total**		
Domaine de la sécurité du matériel	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Dispositifs de sécurité			**1**	**1**			**1**			**1**			**1**			**11**	**0**	**1**
Entretien et soutien du matériel			**1**	**1**			**1**			**1**			**1**			**10**	**0**	**2**
Contrôle de la qualité		**1**		**1**			**1**			**1**				**1**		**9**	**3**	**0**
Domaine de la sécurité des logiciels	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Normes de conception, élaboration, entretien, contrôle de la qualité et essais de réception	**1**			**1**			**1**			**1**			**1**			**12**	**0**	**0**
Logiciels d'exploitation			**1**	**1**			**1**			**1**			**1**			**11**	**0**	**1**
Gestion des données et de la base de données			**1**	**1**			**1**			**1**			**1**			**11**	**0**	**1**
Logiciels d'application			**1**	**1**			**1**			**1**			**1**			**11**	**0**	**1**
Domaine de la sécurité des communications	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Entretien et soutien des communications (infrastructures de télécommunications)			1	1			1			1			1			**11**	**0**	**1**
Logiciels de communication			**1**	**1**			**1**			**1**			**1**			**11**	**0**	**1**
Protection de l'information transmise sur un réseau de communication	**1**			**1**			**1**			**1**			**1**	**1**		**11**	**2**	**0**

Section sur la prévention, la détection, la correction et l'assurance de la sécurité

Quels sont les éléments de prévention, de détection, de correction et d'assurance que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 8**			**M/O 9**			**M/O 10**			**M/O 11**			**M/O 12**			**Total**		
	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Technologies de Coupe-feu ou de garde-barrière	1			1			1			1			1			**12**	**0**	**0**
Technologies de réseau virtuel privé (RVP)	**1**			**1**	**1**			**1**		**1**			**1**			**7**	**4**	**2**
Technologies de serveur de cache ou proxy	**1**			**1**			**1**			**1**			**1**			**11**	**1**	**0**
Outils ou services d'analyse de vulnérabilités (réseau, serveur et donnée)		**1**		**1**				**1**		**1**				**1**		**6**	**6**	**0**
Outils ou services de détection des intrusions (réseau, serveur et donnée)		**1**		**1**	**1**		**1**			**1**			**1**			**7**	**5**	**1**
Outils ou services de protection des données et des programmes (poste et			**1**	**1**			**1**			**1**					**1**	**8**	**1**	**3**
Outils ou services de surveillance (réseau, serveur, contenu, anti-virus)		**1**		**1**			**1**			**1**			**1**			**9**	**2**	**1**
Outils ou services de journalisation et conciliation des journaux		**1**		**1**			**1**			**1**	**1**		**1**	**1**		**10**	**4**	**0**
Outils ou services de gestion de la sécurité (centralisé, répartis, externe)			**1**	**1**					**1**	**1**					**1**	**7**	**1**	**4**
Outils ou services de garantie de haute disponibilité (technologie de grappe, de partage de charge, de relève)			**1**	**1**					**1**	**1**				**1**		**5**	**4**	**3**
Autres																**0**	**0**	**0**

Section sur l'utilisation d'outils et de services spécialisés favorisant DICAI

Quels sont les outils et services spécialisés que votre M/O utilise ou prévoit utiliser afin d'assurer la sécurité de l'information numérique, des ressources informationnelles et de la ou des PES	**M/O 8**			**M/O 9**			**M/O 10**			**M/O 11**			**M/O 12**			**Total**		
	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR	A	F	SR
Outils ou services d'ICP	1				1		1				1			1		**5**	**6**	**1**
Outils ou services de répertoire			**1**		**1**			**1**		**1**	**1**			**1**		**4**	**8**	**1**
Outils ou services d'ouverture de session simplifiée (serveurs spécialisés, etc.)	**1**			**1**				**1**		**1**				**1**		**5**	**5**	**1**
Outils ou services d'authentification (cartes à puces, jetons, serveurs spécialisés, etc.)	**1**				**1**		**1**				**1**			**1**		**6**	**6**	**1**
Outils ou services de contrôle des accès (certificats d'attributs, jetons, serveurs spécialisés, etc.)		**1**		**1**				**1**			**1**			**1**		**5**	**8**	**0**
Outils ou services de chiffrement (données et sessions)	**1**				**1**		**1**				**1**		**1**	**1**		**6**	**6**	**1**
Outils ou services de contrôle d'intégrité (serveurs, données et sessions)			**1**	**1**			**1**			**1**			**1**	**1**		**6**	**5**	**2**
Outil ou service de gestion du consentement			**1**		**1**			**1**		**1**				**1**		**1**	**8**	**3**
Autres																**0**	**0**	**0**

Annexe D

Normes et standards liés à la sécurité

Normes et standards de sécurité généraux

ISO/IEC 13335 - Technologies de l'information - Lignes directrices pour la gestion de la sécurité des technologies de l'information (TI) : La norme ISO/IEC 13335 est un guide pour la gestion de la sécurité des technologies de l'information. Elle compte quatre parties distinctes soit :

Partie 1 – Concepts et modèles pour la sécurité des TI

Partie 2 – Gestion et planification de la sécurité des TI

Partie 3 – Techniques pour la gestion de la sécurité des TI

Partie 4 – Sélection de sauvegardes

ISO/IEC 17799 - Technologies de l'information - Code de pratique pour la gestion de sécurité d'information : Publiée pour la première fois en décembre 2000 d'après la norme BS7799 v2, la norme ISO 17799 est un standard de sécurité extrêmement complet. Elle est organisée autour de dix sections principales touchant aussi bien les aspects organisationnels, logistiques que techniques de la sécurité de l'information numérique. Ses sections couvrent les domaines suivants :

1. Planification de la continuité des affaires
2. Contrôle d'accès aux systèmes
3. Développement et entretien de systèmes
4. Sécurité physique et environnementale
5. Conformité aux lois, politiques, standards, engagements contractuels, etc.
6. Sécurité du personnel
7. Organisation de la sécurité
8. Gestion des ordinateurs et des réseaux
9. Classification et contrôle des actifs
10. Politique de sécurité

ISO 7498-2 - Systèmes de traitement de l'information - Interconnexion de systèmes ouverts - Modèle de référence de base - Partie 2: Architecture de sécurité : La seconde partie de la norme ISO 7498 (le fameux modèle OSI) élargit son champ d'application afin de couvrir les communications sûres entre systèmes ouverts. Elle identifie des services et des mécanismes de sécurité de base et leur placement approprié pour toutes les couches du Modèle de référence de base et définit les relations architecturales entre les services et mécanismes de sécurité et le Modèle de référence de base.

« Critères communs » ou ISO/IEC 15408 - Technologies de l'information - Techniques de sécurité - Critères d'évaluation pour la sécurité TI : Les « Critères communs », qui font l'objet d'une normalisation à l'échelle internationale (ISO/IEC 15408), définissent un ensemble d'exigences, dont la validité est connue, et qui peuvent être utilisées pour établir les exigences de sécurité de futurs produits et systèmes.

Normes et standards liés à la fonction d'intégrité

ISO/IEC 10181-6 - Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres de sécurité pour les systèmes ouverts: Cadre d'intégrité : Le standard ISO/IEC 10181-6 traite de l'intégrité des données, autant au niveau de la localisation que du transfert ou de la gestion de l'information. Plus spécifiquement, ce standard définit le concept de l'intégrité des données, identifie les classes de mécanismes d'intégrité, identifie les infrastructures pour chaque classe de mécanismes, identifie la gestion nécessaire pour supporter les classes de mécanismes d'intégrité et définit les interactions entre les mécanismes d'intégrité et les autres mécanismes de sécurité.

ISO/IEC 9797 - Technologies de l'information - Techniques de sécurité - Codes d'authentification de message (MAC) - Partie 1: Mécanismes utilisant un cryptogramme bloc : Le standard ISO/IEC 9797 spécifie une méthode d'utilisation d'une clé et d'un algorithme de chiffrement afin de calculer une somme de contrôle cryptographique. Cette méthode peut être utilisée comme un mécanisme d'intégrité afin de détecter si des données n'ont pas été altérée de façon non-autorisée.

ISO/IEC 10118 - Technologies de l'information - Techniques de sécurité - Fonctions de brouillage : Ce standard spécifie des fonctions de hachage applicables entre autres à l'intégrité des données.

FIPS PUB 180-1 : Le standard FIPS PUB 180-1 spécifie un algorithme de hachage, SHA-1, permettant de traiter une représentation condensée d'un message ou d'un fichier.

Normes et standards liés à la fonction d'irrévocabilité

ISO/IEC 10181-4 - Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres de sécurité dans les systèmes ouverts: Cadre de non-répudiation : Le standard ISO/IEC 10181-4 définit le concept de l'irrévocabilité (non-répudiation), identifie les services généraux de l'irrévocabilité, identifie les mécanismes possibles permettant de livrer ces services et identifie la gestion nécessaire pour supporter les services et mécanismes d'irrévocabilité.

ISO/IEC 13888 - Technologies de l'information - Techniques de sécurité - Non-répudiation : Ce standard spécifie certains mécanismes utilisant des techniques asymétriques et symétriques pour la réalisation de services spécifiques d'irrévocabilité.

Normes et standards liés à la fonction d'identification et d'authentification

ISO/IEC 10181-2 - Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres de sécurité pour les systèmes ouverts: Cadre d'authentification : Ce standard définit les concepts de base de l'authentification, identifie les classes de mécanismes d'authentification, définit les services pour ces classes de mécanismes, identifie les besoins fonctionnels des protocoles pour supporter ces classes de mécanismes, identifie les infrastructures pour chaque classe de mécanismes et identifie les exigences de gestion générale pour l'authentification.

ISO/IEC 7816 - Technologies de l'information - Cartes d'identification - Cartes à circuit(s) intégré(s) à contacts : Standards pour les cartes à puce définissant la résistance électrique, le positionnement des contacts électriques, les commandes reconnues par les cartes et le protocole de

communication entre les cartes à puce et les lecteurs de cartes. Les commandes du standard ISO/IEC 7816 sont incluses en totalité ou en partie dans la majorité des cartes à puce.

HA-API - Human Authentication API : HA-API est un API générique conçu pour permettre l'intégration de la biométrie à l'intérieur d'applications nécessitant un processus d'identification.

P1363 de l'IEEE - IEEE Standard Specifications for Public Key Cryptography : P1363 de l'IEEE est un nouveau standard qui vise à fournir une couverture complète des techniques bien établies de chiffrement de clé publique. Le projet a produit une version de travail (version finale non encore disponible publiquement) couvrant les techniques de chiffrement de clés publiques. Un addenda (P1363a) visant à ajouter d'autres techniques de chiffrement est présentement en développement. Ce projet est étroitement lié avec les standards émergents de chiffrement à clé publique pour le monde bancaire de l'ANSI et les révisions récentes des documents PKCS de RSA Laboratories.

PKCS de RSA - Public-Key Cryptography Standards : PKCS est un ensemble de standards pour le chiffrement d'ICP développés par RSA Laboratories en collaboration avec un consortium informel incluant originalement Apple, Microsoft, DEC, Lotus, Sun et le MIT. En plus d'être supporté par ISO, l'IETF (à l'intérieur des standards SET, S/MIME, SSL et PKIX) et l'ANSI, PKCS est supporté par plusieurs fournisseurs de solutions ICP tels que Entrust, Baltimore et Verisign. Les standards publiés sont PKCS #1, #3, #5, #7, #8, #9, #10 #11, #12, et #15. PKCS #13 et #14 sont présentement en développement. PKCS #11 est un standard largement reconnu pour l'intégration des cartes à puce aux applications de plusieurs vendeurs.

PKIX de l'IETF - Public-Key Infrastructure (X.509) : Le standard PKIX couvre l'utilisation des certificats X.509 et des listes de révocation des certificats (CRL) et définit les protocoles ICP associés (gestion et validation des certificats). Ce standard est supporté par la plupart des fournisseurs de solutions ICP. Certains fournisseurs tels qu'Entrust et Verisign ont même contribué à l'établissement de ce standard en développant entre autres une série de RFC pour l'IETF (2510, 2511, 2559, 2560 et 2587 par Entrust ; 2459, 2511, 2527 et 2560 par Verisign).

X.509 de l'UIT - Technologies de l'information - Interconnexion des systèmes ouverts - L'annuaire: cadre d'authentification : La recommandation X.509 de l'Union internationale des télécommunications (UIT) spécifie les services d'authentification des répertoires X.500 (voir plus bas), de même que la syntaxe des certificats X.509 (incluant les certificats d'attributs). X.509 définit aussi une syntaxe pour la liste de révocation des certificats (CRL). Le protocole X.509, de même que les certificats basés sur cette norme, sont très répandus sur le marché et sont supportés par un certain nombre de protocoles (ex. SSL, PKCS, PKIX) et la presque totalité des fournisseurs de solutions d'ICP.

SPKI de l'IETF – Simple PKI : Le schéma de certificat Simple PKI, qui inclut la proposition de création de certificat à clé publique *Simple Distributed Security Infrastructure* (SDSI), est en partie une réponse à la complexité croissante du protocole X.509. Il adopte ainsi une notation d'encodage plus simple que celle utilisée par X.509 (ASN.1) et délaisse un certain nombre d'attributs inclus dans le X.509 tels que les politiques de certificat, les contraintes et la gestion du cycle de vie des clés. Le protocole SPKI/SDSI possède un potentiel intéressant, principalement dans des environnements fermés. Cependant, il ne répond pas à plusieurs questions importantes touchant la responsabilité, l'application des politiques et l'auditabilité dans des environnements de commerce électronique.

XML Signature du World Wide Web Consortium : Syntaxe conforme à XML permettant de représenter des signatures numériques et des procédures pour traiter et vérifier de telles signatures. La norme de syntaxe et de traitement des XML Signature est à l'état de « Candidate Recommandation » au W3C et un *Request for Comments* (RFC) a été déposé devant l'IETF.

S2ML - Security Services Markup Language : S2ML est un protocole de sécurisation des échanges basé sur XML qui permet l'interopérabilité des applications de sécurisation dont celles d'authentification par la signature électronique. Il supporte différents corpus XML existants comme BizTalk de Microsoft et ebXML, défendu par l'Oasis et les Nations-Unis. S2ML compte sur des promoteurs tels que Netegrity (le créateur), Art Technology, Bowstreet, Commerce One, Jamcracker, Oracle, PricewaterhouseCoopers, Sun, Tibco, VeriSign et webMethods. Ce standard potentiel est encore à l'état de document de travail.

XKMS – XML Key Management Specification : Développé par Microsoft, Verisign et webMethods, XKMS est une série de protocoles pour la distribution et l'enregistrement des clés publiques qui sont particulièrement appropriés pour être utilisés en conjonction avec XML Signature et XML Encryption. Un objectif clé de XKMS est de minimiser la complexité d'implantation des applications en leur permettant de devenir des clients et ainsi de les protéger de la complexité et de la syntaxe de l'ICP sous-jacente. Cette ICP peut être basée sur différentes spécifications telles que X.509/PKIX, SPKI ou PGP. N'ayant été adopté à l'heure actuelle par aucun organisme de standardisation, XKMS n'a pas encore le statut de norme ou de standard. Cependant, outre leurs instigateurs, plusieurs autres fournisseurs de solutions de sécurité se sont engagés à supporter ces protocoles dont Entrust, Hewlett Packard, IBM et RSA Security.

Format de certificat WTLS du WAP Forum : Le WAP Forum a développé pour les fins d'inclusion au standard WTLS (voir plus bas) un nouveau format de certificat qui est l'équivalent logique de la version 1 du standard X.509. Le certificat WTLS utilise cependant un système d'encodage plus simple que celui inclus dans le X.509 (ASN.1). Ce nouveau format de certificat est communément utilisé pour les certificats de serveur WTLS en raison du fait qu'il est plus facilement transportable et utilisable par des appareils possédant des ressources limitées tels que les téléphones cellulaires.

Kerberos : Développé au MIT dans le cadre du projet Athena, Kerberos est principalement un serveur d'authentification externe. Il permet donc à un correspondant de s'assurer de l'identité de son interlocuteur. Kerberos fournit également des moyens de protéger la confidentialité et l'intégrité des données (chiffrement). Kerberos est entre autres supporté par Windows 2000.

X.500 de l'UIT et de ISO - Technologies de l'information - Interconnexion des systèmes ouverts - L'Annuaire: Vue d'ensemble des concepts, modèles et services : Les standards X.500 développé par l'Union internationale des télécommunications et l'Organisation mondiale de normalisation ont été conçus dans le but de supporter des services de répertoires distribués à utilisations multiples. Les répertoires X.500 peuvent agir comme source d'information sur les gens, les composantes réseau, les applications logicielles ou sur d'autres systèmes. Les répertoires X.500 sont aussi utilisés pour le stockage et la distribution de certificats à clé publique. Malgré sa polyvalence, le niveau d'adoption des standards X.500 n'est pas celui qu'on attendait. La technologie est complexe et ainsi coûteuse à implanter et à déployer.

DAP – Directory Access Protocol : Le protocole d'accès aux services de répertoires X.500 considéré comme trop complexe, a été remplacé par le protocole LDAP.

LDAP de l'IETF – Light Directory Access Protocol : Pour aborder ce problème du service annuaire DAP qui, d'un point de vue pratique, était trop complexe à mettre en œuvre, l'université du Michigan (et par la suite l'IETF) a élaboré une version plus simple du DAP en vue d'une utilisation sur Internet, le protocole simplifié d'accès annuaire (service annuaire LDAP). LDAP offre de nombreuses fonctionnalités de base du DAP et on peut l'utiliser pour interroger des données d'annuaires exclusifs aussi bien que d'un service ouvert X.500. La plupart des fournisseurs importants de logiciels de courrier électronique et de services de répertoires se sont montrés intéressés par LDAP, qui est devenu rapidement le véritable protocole de répertoire utilisé pour Internet.

Normes et standards liés à la fonction d'habilitation/contrôle d'accès

ISO/IEC 10181-3 - Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres de sécurité pour les systèmes ouverts: Cadre de contrôle d'accès : Ce standard définit les concepts de base du contrôle d'accès, démontre comment ces concepts de base peuvent être raffinés pour supporter des services et mécanismes de contrôle d'accès connus, définit ces services et les mécanismes de contrôle d'accès correspondants, identifie les besoins fonctionnels afin que les protocoles supportent ces services et mécanismes, identifie les exigences de gestion générale pour supporter ces services et mécanismes et définit les interactions entre les mécanismes de contrôle d'accès et les autres mécanismes de sécurité.

X.509 de l'UIT : voir « Normes et standards liés à la fonction d'identification/authentification ».

SPKI de l'IETF : voir « Normes et standards liés à la fonction d'identification/authentification ».

X.500 de l'UIT : voir « Normes et standards liés à la fonction d'identification/authentification ».

DAP : voir « Normes et standards liés à la fonction d'identification/authentification ».

LDAP : voir « Normes et standards liés à la fonction d'identification/authentification ».

IPSec de l'IETF - IP Security *:* IPSec est un ensemble de standards ouverts qui permettent l'échange sécurisé de données de même que l'intégrité et l'authentification de ces données. IPSec fournit ces services de sécurité au niveau de la couche IP (niveau réseau) et permet de sécuriser plusieurs flux de données entre deux hôtes, deux passerelles de sécurité ou une passerelle et un hôte. Il s'agit du protocole de choix de la plupart des fournisseurs de solutions de sécurisation du trafic (dont les coupe-feu) tels que Cisco, Checkpoint, Alcatel, Lucent, 3Com, Baltimore Technologies, etc. Il ne supporte cependant pas les protocoles réseaux propriétaires tels que IPX.

Normes et standards liés à la fonction de confidentialité

ISO/IEC 10181-5 - Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres de sécurité pour les systèmes ouverts: Cadre de confidentialité : Le standard ISO/IEC 10181-5 traite de la confidentialité de l'information, autant au niveau de la localisation que du transfert ou de la gestion de l'information. Plus spécifiquement, ce standard définit les concepts de base de la confidentialité, identifie les classes de mécanismes de confidentialité, classifie et identifie les infrastructures pour chaque classe de mécanismes, identifie la gestion nécessaire pour supporter les classes de mécanismes d'intégrité et définit les interactions entre les mécanismes de confidentialité et les autres mécanismes de sécurité.

L2TP - Layer 2 Tunnelling Protocol : L2TP est un protocole permettant la sécurisation du trafic à l'intérieur d'un RPV. Il est la résultante d'une fusion entre le protocole RPV de Microsoft, « Point-to-Point Tunneling Protocol » (PPTP) et celui de Cisco, *Layer 2 Forwarding* (L2F). Ce protocole possède une popularité certaine auprès des organisations qui supportent des protocoles non-IP, mais possède de faibles capacités d'authentification et de support des RPV de grande taille. Il est favorablement remplacé par le protocole IPSec du IETF.

SSL/TLS de l'IETF - Secure Sockets Layer/Transport Layer Security : Le standard SSL est un protocole de sécurité Internet pour les connexions point-à-point. Il fournit une protection contre la surveillance électronique, la manipulation et la contrefaçon des données. Contrairement à IPSec qui

sécurise les données en créant un canal sécurisé sur le réseau où elles circulent (niveau réseau), SSL sécurise les données uniquement entre deux applications (niveau transport). Ce standard de sécurité est certainement le plus répandu sur Internet. On l'utilise généralement pour chiffrer des données liées aux processus d'achat électronique telles que des données nominatives, des numéros de carte de crédit, etc. TLS est le nom donné à SSL par l'IETF lorsque cette dernière l'a reprise des mains de son inventeur, Netscape. TLS contient quelques modifications, mais ne représente pas une avancée significative par rapport à SSL.

IPSec de l'IETF : voir « Normes et standards liés à la fonction d'habilitation/contrôle d'accès ».

S/MIME de l'IETF - Secure/MIME : Le standard S/MIME, une nouvelle version du protocole de messagerie électronique MIME, est un service de messagerie électronique sécurisé (chiffré). Développé initialement par un groupe de travail mené par la compagnie RSA Security, S/MIME est maintenant supporté par tous les principaux fournisseurs de solutions de messagerie électronique. Le standard S/MIME a gagné de la popularité par rapport aux propositions de messagerie sécurisée des concurrents (*Pretty Good Privacy*, *Privacy Enhanced Mail*, *X.400 Security*, *Message Security Protocol*) principalement en raison du fait qu'il est construit sur la base des populaires standards PKCS.

XML Encryption du World Wide Web Consortium : Processus pour chiffrer et déchiffrer un contenu numérique (incluant des documents XML et des parties de ceux-ci) et syntaxe XML utilisée pour représenter le contenu chiffré et l'information permettant au destinataire de le déchiffrer.

WTLS du ASP Forum - Wireless Transport Layer Security : Le protocole WTLS est une partie du standard de l'industrie sans fil, Wireless Application Protocol (WAP). WTLS est un proche parent du standard SSL/TLS. Il fournit les mêmes fonctionnalités de base, mais avec quelques attributs optimisés pour la faible bande passante de l'environnement sans fil.

Norme et standards liés à la fonction de disponibilité

Aucun

Normes et standards liés à la fonction de surveillance

ISO/IEC 10181-7 - Technologies de l'information - Interconnexion de systèmes ouverts (OSI) - Cadres de sécurité pour les systèmes ouverts: Cadre d'audit et d'alarmes de sécurité : Le but de ce standard portant sur les alarmes et les audits est de s'assurer que les événements reliés à la sécurité des systèmes soit gérés en accord avec les politiques de sécurité. Plus spécifiquement, ce standard définit les concepts de base des alarmes et audits de sécurité, fournit un modèle général des alarmes et audits de sécurité et définit les interactions entre le service d'alarme et d'audit et les autres services de sécurité.

SNMP - Simple Network Management Protocol : SNMP est un protocole de transmission dérivé de TCP/IP qui gouverne la gestion des réseaux et le monitorage des équipements réseaux. SNMP possède cependant certaines lacunes de sécurité qui incitent les fournisseurs de ces solutions d'administration à proposer plutôt des protocoles propriétaires.

RMON – Remote Monitoring : Le protocole RMON est un protocole de gestion à distance des réseaux qui permet l'interopérabilité multi-vendeurs entre des solutions de monitorage et des postes de gestion.

RMON2 - Remote Monitoring 2 : Extension à SNMP permettant aux applications d'administration de recueillir des données provenant de senseurs d'analyse de réseau. Ces données incluent le niveau de trafic par application entre les circuits de données et entre deux senseurs.

Normes et standards liés à la fonction d'administration

WBEM/CIM du Distributed Management Task Force : Common Information Model est un modèle conceptuel d'information visant à décrire l'information d'administration. Ceci permet l'échange d'informations entre les systèmes d'administration de différents fournisseurs et les applications. Ce standard est activement supporté entre autres par Microsoft (Windows 2000), Sun (Solaris), Intel et IBM (Tivoli).

SNMP : Voir « Normes et standards liés à la fonction de surveillance ».

RMON : Voir « Normes et standards liés à la fonction de surveillance ».

RMON2 : Voir « Normes et standards liés à la fonction de surveillance ».

Annexe E

Liste des membres du Comité d'orientation stratégique sur la sécurité (COSS) et des participants aux ateliers de consultation

Membres du COSS au 4 juin 2001

Organisation	Participants
ANQ	Marc-André Leclerc
CNT	Alain Chassé
CSST	Guy Rochette
Hydro-Québec	Kathleen Potvin
IGIF	Jean-Pierre Maillé
Loto-Québec	Yves Leblanc
MFQ (Contrôleur)	Alain Fortin
MJQ (RDPRM)	Jeannne Proulx Hélène Gingras
MRCI	Marc Lafrance Guy Lavigne
MRQ	Michel Leblanc
MSSS	Claude Lévesque
OPC	Yolande Côté
RAMQ	Roger Girardeau
SAAQ	Claude Gélinas
SCT (SSIGRI)	Michel Després
SSSG (DGSIG)	Normand Hogue
SSSG (DGT)	Gilbert Coutu
SQ	Jean-Guy Pelletier Denis Rioux

Groupe PES

Organisation	Participant
ANQ	Micheline Bélanger
CSST	Jean-Luc Duval François Maranda Claude Lavoie
MCC	Jean-Yves Beaudoin
MFQ – Contrôleur des finances	Michel Lambert

	Serge Riverin
MJQ	Georgine Shum Tim
MRCI	Francine Thomas Denyse Roussel
MRQ	Bruno Fortier Gérald Nadeau
MSS	Denis Carrier Claude Duchemin
MSSS	Claude Lévesque Bernard Roy
RAMQ	Jacques Blouin
RRQ	Pierre Bélisle
SAAQ	Stéphane Cormier Mario Trudel Martine Boucher
SCT	Louise Thiboutot François Lepage
SCT – DGSIG	Marc Plamondon
SCT – DGT	Gaétan Laberge
SCT – GIRES	Thérèse Blanchet
SQ	Jean-Guy Pelletier Raymond Gascon

Groupe Portrait et besoins

Organisation	**Participant**
CSST	Alain Brochu
MFQ – Contrôleur des finances	Christine Cameron Jean-Guy Giguère
MRCI – DSAIPRP	Denyse Roussel
MRN	Claude Taillon
MRQ	Jacques Clouston
MSS	Claude Duchemin
RAMQ	Jacques Blouin
SAAQ	Mario Trudel
SCT	Pierre Sasseville
SCT – DGSIG	Normand Hogue

Organisation	Participant
SCT – DGT	Gaetan Laberge

Groupe ICPG

Organisation	Participant
Conseil Exécutif	Marc Bédard
Hydro-Québec	Monelle JeuneHomme
Loto-Québec	Harold Côté Yves Leblanc
MFQ – Contrôleur des finances	Jean Rhéaume
MJQ	Georgine Shum Tim
MRQ	Patrick Tremblay
RAMQ	Michelle Quintal
SAAQ	Michel Bourassa
SCT	Michel Cloutier Lise Murphy Michel Matte
SCT – DGT	Pierre-Paul Tremblay
SQ	Bernard Dionne

Groupe Répertoire et GIRES

Organisation	Participant
MFQ – Contrôleur des finances	Jean Rhéaume Denis Aubé
MSSS	Robert Brochu Bernard Roy
SAAQ	Jean-Louis Deneault
SCT	René Lortie Richard Parent Daniel Pelletier
SCT – GIRES	Thérèse Blanchet Daniel Dore Denis Turcotte

Annexe F

Stratégies d'affaires et exigences architecturales

Stratégies d'affaires et exigences architecturales

QUALITÉ DE LA PRESTATION DE SERVICES AUX INDIVIDUS	
Stratégies d'affaires	**Exigences architecturales**
Libre-choix : ▪ Choix du moyen de communication pour transiger avec l'Administration publique.	La prestation électronique de services prévoit : ▪ Une possibilité d'accès en mode libre-service par l'ensemble des clientèles à qui sont destinés les services ; ▪ Une assistance permettant de recourir à un mode alternatif de services.
Disponibilité et accessibilité : ▪ Disponibilité pratiquement continue du service ▪ Soutien 24 heures sur 24, 7 jours / semaine lorsque requis ▪ Accessibilité à l'ensemble du territoire sous réserve de la disponibilité des infrastructures appropriées	▪ La prestation électronique de services est adaptée aux différents types de clientèles maximisant ainsi son utilisation et l'atteinte des résultats visés par les services. ▪ La prestation électronique de services prévoit : ▫ Une possibilité d'accès en mode libre-service par l'ensemble des clientèles à qui sont destinés les services ; ▫ Une disponibilité élargie des heures de services ; ▫ Une assistance permettant de recourir à un mode alternatif de services ; ▫ Des mécanismes adéquats de soutien aux utilisateurs. ▪ *La prestation électronique de services doit être supportée par des mécanismes qui permettent d'assurer la sécurité de l'information numérique en tout temps et sur l'ensemble du territoire.*
Simplicité et convivialité : ▪ Niveau de convivialité accrue pour l'utilisateur ▪ Prestation dans la langue de l'utilisateur ▪ Personnalisation du service selon les besoins et le contexte de l'utilisateur ▪ Soutien à l'utilisateur adapté à ses spécificités	▪ La prestation électronique de services est conçue dans la perspective des individus et des entreprises, en tenant compte des événements qui les touchent durant leur vie ou leurs activités. ▪ Les services sont mis en place dans un souci de simplification et d'intégration des mécanismes de communication et de transactions avec les individus. ▪ La prestation électronique de services prévoit des mécanismes adéquats de soutien aux utilisateurs. ▪ Les moyens mis en place par l'Administration publique pour la prestation électronique de services sont arrimés à ceux de l'entreprise privée dans un souci de mieux servir les individus tout en optimisant l'utilisation des ressources. ▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la*

QUALITÉ DE LA PRESTATION DE SERVICES AUX INDIVIDUS	
Stratégies d'affaires	**Exigences architecturales**
	prestation électronique de services.
Efficacité : ▪ Rapidité de réponse aux requêtes de l'utilisateur ▪ Diligence de livraison des produits et services demandés ▪ Fiabilité et pertinence du résultat obtenu	▪ Les individus et les entreprises ont un accès simplifié aux dossiers que maintiennent les organismes gouvernementaux à leur égard. ▪ Les informations gouvernementales de nature publique sont rendues plus facilement disponibles aux individus et aux entreprises. ▪ La prestation électronique de services prévoit une livraison rapide des réponses et des résultats. ▪ Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place contribuent à la qualité des services aux individus et aux entreprises. ▪ *Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place doivent permettre d'assurer l'intégrité et l'irrévocabilité lorsque nécessaire.*
Équité : ▪ Niveau de service acceptable pour tout utilisateur, peu importe l'endroit d'où est requis le service	▪ La prestation électronique de services est adaptée aux différents types de clientèle maximisant ainsi son utilisation et l'atteinte des résultats visés par les services. ▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.*
Sécurité : ▪ *Sécurité garantie (adéquate) des transactions (communications) électroniques* ▪ *Protection adéquate des renseignements personnels*	▪ *L'environnement de soutien à la prestation électronique de services est sécurisé en fonction du cadre légal et réglementaire en vigueur au Québec, et de manière à inspirer confiance à l'utilisateur.*
Avantages économiques : ▪ Potentiel d'une tarification de services moins élevée ▪ Avantage économique pouvant résulter d'un service plus rapide et plus efficace	▪ La prestation électronique de services prévoit une livraison rapide des réponses et des résultats. ▪ Les composantes d'information et d'application les plus largement utilisées sont mises en commun et d'autres partagées afin de bénéficier d'économies d'échelle et de réduire les délais de mise en œuvre des services.

QUALITÉ DE LA PRESTATION DE SERVICES AUX INDIVIDUS	
Stratégies d'affaires	**Exigences architecturales**
	▪ Les moyens mis en place par l'Administration publique pour la prestation électronique de services sont arrimés à ceux de l'entreprise privée dans un souci de mieux servir les individus tout en optimisant l'utilisation des ressources. ▪ Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place contribuent à la qualité des services aux individus et aux entreprises et à la performance de l'Administration publique.

STRATÉGIES D'AFFAIRES ET EXIGENCES ARCHITECTURALES

PERFORMANCE DE L'ADMINISTRATION PUBLIQUE	
Stratégies d'affaires	**Exigences architecturales**
Efficacité des employés : ▪ Accroissement de l'efficacité dans un contexte de réorganisation du travail	▪ Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place contribuent à la performance de l'Administration publique. ▪ *Les mécanismes de sécurité doivent permettre d'assurer la protection des renseignements personnels durant tout le cycle de vie de l'information.*
Compétitivité du gouvernement : ▪ Réduction des coûts globaux de fonctionnement ▪ Amélioration de l'expertise dans les nouvelles technologies ▪ Projection d'une image d'efficacité et de compétence	▪ Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place contribuent à la qualité des services aux individus et aux entreprises et à la performance de l'Administration publique. ▪ En tant que levier de développement, la prestation électronique de services permet notamment de rendre disponible : ▫ Des informations et des services visant le mieux-être des individus ; ▫ Des services et des contenus projetant une image de modernité et d'avant-garde qui rendent le Québec attrayant aussi bien localement qu'à l'étranger. ▫ *Des mécanismes reconnus et harmonisés en matière de sécurité de l'information numérique.*

PERFORMANCE DE L'ADMINISTRATION PUBLIQUE	
Stratégies d'affaires	**Exigences architecturales**
Réduction des coûts d'opération : ▪ Coûts globaux de fonctionnement ▪ Économie d'échelle ▪ Coût de prestation des services ▪ Coût de gestion des programmes	▪ Les composantes d'information et d'application les plus largement utilisées sont mises en commun et d'autres sont partagées afin de bénéficier d'économies d'échelle et de réduire les délais de mise en œuvre des services. ▪ Les moyens mis en place par l'Administration publique pour la prestation de services sont arrimés à ceux de l'entreprise privée dans un souci de mieux servir les individus tout en optimisant l'utilisation des ressources. ▪ Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place contribuent à la qualité des services aux individus et aux entreprises et à la performance de l'Administration publique. ▪ La prestation électronique de services tire le meilleur profit des systèmes et des infrastructures existantes tout en favorisant une modularité des applications d'avant-plan et d'arrière-plan ▪ *Les mécanismes de sécurité doivent présenter un rapport risques/coûts acceptable.*
Contribution du secteur privé : ▪ Partenariats avec l'entreprise privée	▪ Les moyens mis en place par l'Administration publique pour la prestation électronique de services sont arrimés à ceux de l'entreprise privée dans un souci de mieux servir les individus tout en optimisant l'utilisation des ressources. ▪ *L'arrimage entre l'Administration publique et l'entreprise privée doit se faire dans un environnement sécurisé afin de protéger les renseignements personnels et la vie privée.*
Atteinte des résultats : ▪ Atteinte des résultats des programmes gouvernementaux ▪ Disponibilité d'indicateurs de gestion	▪ La prestation électronique de services est adaptée aux différents types de clientèle maximisant ainsi son utilisation et l'atteinte des résultats visés par les services. ▪ La prestation électronique de services tire le meilleur profit des systèmes et des infrastructures existantes tout en favorisant une modularité des applications d'avant-plan et d'arrière-plan ▪ L'architecture de la prestation électronique des services est fondée sur les normes les plus ouvertes de l'industrie afin de maximiser son évolutivité.

PERFORMANCE DE L'ADMINISTRATION PUBLIQUE	
Stratégies d'affaires	**Exigences architecturales**
Partage entre les organisations : ▪ Intégration de services multi-organisations ▪ Économies d'échelle ▪ Services communs	▪ Les services sont mis en place dans un souci de simplification et d'intégration des mécanismes de communication et de transactions avec les individus. ▪ Les individus et les entreprises ont un accès simplifié aux dossiers que maintiennent les organismes gouvernementaux à leur égard. ▪ *Les solutions envisagées pour simplifier et intégrer les mécanismes de communication électronique doivent permettre d'assurer la sécurité de l'information numérique.*

STRATÉGIES D'AFFAIRES ET EXIGENCES ARCHITECTURALES

LEVIER DE DÉVELOPPEMENT SOCIAL, CULTUREL ET ÉCONOMIQUE	
Stratégies d'affaires	**Exigences architecturales**
Adoption des nouvelles technologies par les individus : ▪ Utilisation accrue des NTIC ▪ Échanges et transactions avec le gouvernement	▪ La prestation électronique de services est adaptée aux différents types de clientèle maximisant ainsi son utilisation et l'atteinte des résultats visés par les services. ▪ Les informations gouvernementales de nature publique sont rendues plus facilement disponibles aux individus et aux entreprises. ▪ Les individus et entreprises ont un accès simplifié aux dossiers que maintiennent les organismes gouvernementaux à leur égard. ▪ *L'environnement de soutien à la prestation électronique de services est sécurisé de manière à respecter le cadre légal et réglementaire en vigueur au Québec, et inspirer confiance à l'utilisateur.* ▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.*
Adoption des nouvelles technologies par les entreprises : ▪ Utilisation et développement de l'autoroute de l'information ▪ Commerce électronique	▪ La prestation électronique de services est adaptée aux différents types de clientèle maximisant ainsi son utilisation et l'atteinte des résultats visés par les services. ▪ Les individus et entreprises ont un accès simplifié aux dossiers que maintiennent les organismes gouvernementaux à leur égard.

LEVIER DE DÉVELOPPEMENT SOCIAL, CULTUREL ET ÉCONOMIQUE	
Stratégies d'affaires	**Exigences architecturales**
	▪ *L'environnement de soutien à la prestation électronique de services est sécurisé de manière à respecter le cadre légal et réglementaire en vigueur au Québec, et inspirer confiance à l'utilisateur.* ▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services..*
Maximiser l'effet de levier des investissements consentis : ▪ Mieux-être de la population ▪ Culture ▪ Éducation ▪ Échanges commerciaux ▪ Vie démocratique	En tant que levier de développement, la prestation électronique de services permet notamment de rendre disponibles : ▪ Des informations et des services visant le mieux-être des individus ; ▪ Des services et des contenus éducatifs et culturels en français ; ▪ Des informations, des services et des infrastructures stimulant l'activité économique au Québec.
Augmentation et amélioration des contenus : ▪ Francophones ▪ Sociaux ▪ Culturels ▪ Éducatifs	▪ Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place contribuent au développement social, culturel, éducatif et économique du Québec.
Promotion du Québec : ▪ Localement et à l'étranger ▪ Image de modernité	▪ En tant que levier de développement, la prestation électronique de services permet notamment de rendre disponible des services et des contenus projetant une image de modernité et d'avant-garde qui rendent le Québec attrayant aussi bien localement qu'à l'étranger. ▪ *Les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.* ▪ *La prestation électronique de services doit être supportée par des mécanismes qui permettent d'assurer la sécurité de l'information numérique en tout temps et sur l'ensemble du territoire.*

LEVIER DE DÉVELOPPEMENT SOCIAL, CULTUREL ET ÉCONOMIQUE	
Stratégies d'affaires	**Exigences architecturales**
Développement de l'industrie des TIC au Québec : ▪ Croissance ▪ Développement d'une main-d'œuvre spécialisée	▪ Les projets de prestation électronique de services et les systèmes qu'ils permettent de mettre en place contribuent au développement social, culturel, éducatif et économique du Québec. ▪ En tant que levier de développement, la prestation électronique de services permet notamment de rendre disponible des informations, des services et des infrastructures stimulant l'activité économique au Québec.
Rehaussement du potentiel d'exportation de l'industrie des TIC : ▪ Normes internationales ▪ Produits et services d'avant-garde	▪ *L'architecture de la sécurité de la prestation électronique des services est fondée sur les normes les plus ouvertes de l'industrie en matière de sécurité afin de maximiser son évolutivité.* ▪ En tant que levier de développement, la prestation électronique de services permet notamment de rendre disponible des services et des contenus projetant une image de modernité et d'avant-garde qui rendent le Québec attrayant aussi bien localement qu'à l'étranger.