Segment sécurité

Architecture de sécurité de l'information gouvernementale

Architecture d'entreprise gouvernementale 3.1

Segment sécurité

Architecture de sécurité de l'information gouvernementale

Architecture d’entreprise gouvernementale 3.1

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite en collaboration avec la Direction des communications
du Secrétariat du Conseil du trésor.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – mars 2015
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-72733-0 (en ligne)

Table des matières

Liste des sigles et acronymes

AEG	Architecture d'entreprise gouvernementale
AFNOR	Association française de normalisation
AGSIN	Architecture gouvernementale de sécurité de l'information numérique
ANS	Accord sur les niveaux de service
AOS	Architecture orientée service
API	*Application Programming Interface*
ASI	Architecture de sécurité de l'information
ASIG	Architecture de sécurité de l'information gouvernementale
BYOD	*Bring your own device*
ClicSÉQUR	Service québécois d'authentification gouvernementale
COBIT	*Control Objectives for Information and Related Technology*
DPI	Dirigeant principal de l'information
GIA	Gestion de l'identité et des accès
GQ	Gouvernement du Québec
HTTP	*Hypertexte Transfer Protocol*
IaaS	*Infrastructure as a service*
ICPG	Infrastructure à clés publiques gouvernementale
ISO	Organisation internationale de normalisation
MV	Machine virtuelle
NIST	*National Institute of Standards and Technology*
NTIC	Nouvelles technologies de l'information et de la communication
OP	Organisme public
OS	*Operating system*
OSA	*Open Security Architecture*
PaaS	*Platform as a service*
PAP	Prenez vos appareils personnels
PES	Prestation électronique de services
RI	Ressources informationnelles
RITM	Réseau intégré de télécommunications multimédias

SaaS	*Software as a service*
SAML	*Security Assertion Markup Language*
SCT	Secrétariat du Conseil du trésor
SGQRI	Standards du gouvernement du Québec en ressources informationnelles
SGSI	Système de gestion de la sécurité de l’information
SI	Sécurité de l’information
SLA	*Service Level Agreement*
SSDPI	Sous-secrétariat du dirigeant principal de l'information
TI	Technologies de l’information
TOGAF	*The Open Group Architecture Framework*
URI	*Uniform Resource Identifier*
WIFI	*Wireless Fidelity*
XACML	*Extensible Access Control Markup Language*
XML	*Extensible Markup Language*

Historique des versions

Version de l'AEG	Statut	Modifications
3.0	Novembre 2014	-
3.1	Mars 2015	Publication de la première édition

La version en vigueur est disponible à cette adresse :

http://www.tresor.gouv.qc.ca/ressources-informationnelles/architecture-dentreprise-gouvernementale/

Équipe de réalisation

M. Jean Rhéaume
Secrétariat du Conseil du trésor

M. Yassine Maghlout
Secrétariat du Conseil du trésor

Notes à l'intention du lecteur

Note 1 :	Pour ne pas alourdir le texte, le masculin est utilisé comme générique dans le présent document.
Note 2 :	Les termes « organisme public » et « organisme » désignent un ministère ou un organisme, qu'il soit budgétaire ou autre que budgétaire, ainsi que tout organisme des réseaux de l'éducation, de l'enseignement supérieur ou de la santé et des services sociaux [Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement].
Note 3 :	Bien que les éléments du présent guide soient applicables à la plupart des organismes publics, il convient pour chacun de les adapter à son contexte et aux risques qui lui sont propres.

Résumé

Ce document présente les orientations concernant de la sécurisation de l'architecture d'entreprise gouvernementale et les travaux réalisés à ce jour à partir des différents volets de l'architecture d'entreprise. Il propose aussi des priorités d'action en matière de sécurité afin d'en poursuivre la validation et d'en permettre l'évolution.

Destinataires

Dirigeants principaux de l'information

Responsables organisationnels de la sécurité de l'information

Conseillers organisationnels de la sécurité de l'information

Responsables de l'architecture de sécurité de l'information

Architectes de sécurité de l'information

Conseillers en sécurité de l'information

Spécialistes en sécurité

Gestionnaires

1. Introduction

La Directive sur la sécurité de l'information gouvernementale[1] stipule que les mesures de sécurité sélectionnées par un organisme public doivent être proportionnelles à la valeur de l'information gouvernementale à protéger. Elles sont établies en fonction des risques, de leur probabilité d'occurrence et de leurs conséquences.

La Directive stipule aussi que le ministre ou le dirigeant d'un organisme public doit s'assurer de la mise en œuvre de processus formels de sécurité de l'information. Elle est complétée par trois documents établissant des orientations et des lignes directrices, notamment en matière de gouvernance de la sécurité de l'information.

Dans l'approche stratégique triennale[2], le gouvernement du Québec précise par ailleurs sa vision de l'encadrement de la sécurité de l'information, sur un horizon de dix ans, comme suit :

« L'information gouvernementale bénéficie d'une sécurité optimale, peu importe l'endroit où elle est conservée, manipulée ou transmise. À terme, les organismes publics ont atteint un niveau de maturité où la sécurité de l'information est ancrée dans la culture de l'organisation et où les objectifs, les pratiques et les mesures de performance sont définis, et les processus normalisés, intégrés, documentés et implémentés. Tout risque de sécurité est géré en tenant compte des impacts sur l'ensemble du gouvernement. »

Cet encadrement de la sécurité de l'information s'effectue, d'une part, par le dirigeant principal de l'information (DPI), qui coordonne la mise en œuvre et le suivi de mesures d'encadrement auprès des organismes publics et, d'autre part, par ces derniers, qui ont la responsabilité d'appliquer ces mesures[3].

Par ailleurs, le document d'architecture gouvernementale de sécurité de l'information numérique (AGSIN), publié en 2001, a contribué à soutenir le déploiement concret des services en ligne des organismes publics. En 2006, la portée de la directive sur la sécurité de l'information s'est élargie de telle sorte qu'elle englobe désormais la sécurité de toute l'information gouvernementale, peu importe les supports d'information utilisés.

Depuis, le paysage de la sécurité a considérablement évolué, y compris les éléments qui concernent le cadre légal, les menaces, les normes, les standards et les bonnes pratiques de sécurité. De 2001 à 2015, les menaces et les solutions du domaine de la sécurité de l'information n'ont cessé d'évoluer de façon rapide et soutenue. La sécurisation de l'information est essentielle au succès de la transformation de l'État et au déploiement des solutions retenues afin que le lien de confiance avec l'usager soit renforcé.

Cette vision découle d'une réflexion sur les résultats d'un travail préliminaire portant sur la réalisation d'une étude de contexte en sécurité de l'information. Cette étude proposait principalement une revue des façons de faire actuelles en ingénierie de la sécurité, un inventaire des principaux risques pouvant toucher les environnements gouvernementaux et une analyse d'impact du nouveau cadre gouvernemental en sécurité du gouvernement du Québec.

1. Secrétariat du Conseil du trésor, Directive sur la sécurité de l'information gouvernementale (Version 1.0), janvier 2014.
2. Secrétariat du Conseil du trésor, Approche stratégique triennale 2014-2017 en sécurité de l'information gouvernementale (version 1.0), mai 2013.
3. Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, L.R.Q., c. G-1.03.

1.1 Buts

Ce document vise à proposer une vision afin de déterminer les stratégies nécessaires et d'élaborer les plans des éléments de solution aptes à protéger adéquatement l'ensemble des informations du gouvernement du Québec. Il vise aussi à soutenir les organismes publics dans la conception de leurs propres architectures de sécurité de l'information en harmonie avec la vision gouvernementale.

Les architectures de sécurité de l'information ainsi conçues deviennent la pierre angulaire de programmes de sécurité du gouvernement et des organismes concernés, favorisant des progrès concrets, continus et cohérents avec la vision du gouvernement, avec les objectifs de l'organisation et avec le risque auquel elle est exposée.

1.2 Auditoire

Ce document s'adresse aux :

- ✓ Dirigeants principaux de l'information;
- ✓ Responsables organisationnels de la sécurité de l'information;
- ✓ Conseillers organisationnels de la sécurité de l'information;
- ✓ Responsables de l'architecture de sécurité de l'information;
- ✓ Responsables de l'architecture d'entreprise;
- ✓ Architectes de sécurité de l'information;
- ✓ Spécialistes en sécurité;
- ✓ Gestionnaires.

2. Objectifs et portée

Les principaux objectifs de l'architecture de sécurité de l'information gouvernementale (ASIG) sont d'identifier et d'analyser les éléments architecturaux de haut niveau permettant au SSDPI de promouvoir auprès des organismes publics (OP) une vision commune de la sécurité de l'information, d'une part, et d'autre part, de soutenir la mise en œuvre des grandes orientations gouvernementales associées à l'architecture d'entreprise gouvernementale (AEG).

Cette vision commune doit favoriser la cohérence et la confiance pour la clientèle du gouvernement dans la prestation électronique de services. Elle favorise aussi l'interopérabilité entre les organismes publics ou entre les OP et les fournisseurs lors, entre autres, de la mise en commun et du partage d'actifs informationnels, la gouvernance et le contrôle de gestion lors du recours aux nouveaux modes d'acquisition des ressources en RI (externalisation et infonuagique) et une protection adéquate des informations.

Ce document propose de fournir à l'ensemble des intervenants du gouvernement du Québec œuvrant en RI une vision commune de la sécurité de l'information 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;
- ✓ D'arrimer cette vision aux grandes orientations stratégiques gouvernementales;
- ✓ D'alimenter à terme un plan d'action souple en vue d'une mise en œuvre harmonieuse de l'architecture gouvernementale cible.

La démarche de production de l'ASIG s'inscrit dans un processus itératif d'évolution continue de l'AEG. Celle-ci vise à maintenir la capacité réelle du gouvernement du Québec à protéger ses informations au fil du temps. Le cadre méthodologique de l'AEG devra être adapté, s'il y a lieu, dans ses mécanismes de suivi et d'ajustement de l'architecture, y compris par la mise en œuvre d'une vigie constante, afin qu'il tienne compte de l'évolution continue des façons de faire du gouvernement et de son environnement juridique, humain, organisationnel et technologique.

L'ASIG est un exercice gouvernemental de haut niveau qui vise essentiellement à :

- ✓ Comprendre, définir et illustrer les plans et les éléments de sécurité aptes à protéger les informations du gouvernement du Québec, et ce, quel que soit le support d'information utilisé;
- ✓ Alimenter une stratégie gouvernementale de mise en œuvre de la sécurité de l'information gouvernementale dans l'administration publique québécoise;
- ✓ Dégager les plans et les principes directeurs de sécurité du modèle d'affaires cible de l'AEG;
- ✓ Présenter le modèle de référence de sécurisation de l'information d'une organisation;
- ✓ Fournir un aperçu de haut niveau des processus d'affaires, des services et des informations qui composent la sécurité, et permettre la détermination du potentiel de mise en commun de ceux-ci;
- ✓ Orienter l'organisation et l'évolution des éléments constituants de l'AEG.

Cette architecture de haut niveau, essentielle à la cohérence de l'État en matière de sécurité a pour portée la sécurisation de l'information gouvernementale. L'information visée est celle qu'un ministère ou un organisme détient dans l'exercice de sa mission, que sa conservation soit assurée par lui-même ou par un tiers.

L'ASIG couvre la protection de la disponibilité, de l'intégrité et de la confidentialité des informations de prestation gouvernementale et des autres activités administratives de l'État, quel que soit le support ou le mode de prestation utilisé au gouvernement du Québec, quelle que soit l'organisation publique ou privée concernée, que cette information soit conservée dans un dépôt ou qu'elle soit en circulation, et ce, tout au long du cycle de vie des informations.

La clientèle cible de ce document est l'usager gouvernemental pris au sens large du terme, c'est-à-dire, tout individu, groupe ou entreprise, qui entre en relation avec l'information gouvernementale. Celui-ci comprend les citoyens, les entreprises et leur personnel ainsi que les autres usagers consommateurs de la prestation de services gouvernementale, mais aussi, par extension, tous les employés de l'État et ses partenaires.

Plus spécifiquement, ce projet consiste à :

- ✓ Établir une vision, des orientations et des principes en matière de sécurité conformes à ceux établis par l'AEG et les enrichir;
- ✓ Utiliser un cadre de référence global en sécurité et en architecture de sécurité de l'information basé sur les meilleures pratiques en ce domaine;
- ✓ Revoir la modélisation de la sécurité en ce qui a trait aux mesures, aux fonctions et aux mécanismes de sécurité de l'information, quel que soit le support, dont la prestation électronique des services (PES) et les services Web, en représentant ses principales composantes, ses interrelations
- ✓ Faire ressortir les mesures, les fonctions de sécurité ainsi que les mécanismes de sécurité et les solutions technologiques qui présentent un potentiel de mise en commun, de partage ou de réutilisation à l'échelle gouvernementale, et de cohérence pour la clientèle;
- ✓ Définir des zones de normalisation et des normes ouvertes, *de facto* ou émergentes pertinentes à l'ASIG;
- ✓ Déterminer des priorités d'action concernant la mise en œuvre de la sécurité et convenir des suites à donner.

Le segment sécurité se limite à ne définir que les concepts inhérents à la sécurité. L'identification des composantes de nature commune, partageable et réutilisable 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 ou à la normalisation d'objets particuliers;
- ✓ Procéder à l'analyse coût-avantage inhérente à l'usage d'une composante;
- ✓ Se prononcer quant à l'obligation de faire usage des composantes jugées comme étant essentielles.

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

Finalement, plusieurs éléments ont été pris en compte lors de la réalisation des travaux, notamment :

- ✓ Le contexte légal et normatif gouvernemental;
- ✓ L'architecture gouvernementale de sécurité de l'information numérique en vigueur;
- ✓ Les tendances en architecture de sécurité;
- ✓ L'évolution des normes et des standards en sécurité de l'information;
- ✓ Les préoccupations des responsables du dossier au SCT, exprimées au cours d'un processus de consultation continue;
- ✓ Les travaux de l'AEG;
- ✓ L'expérience et les suggestions de certains organismes publics;
- ✓ Les orientations et les principales réalisations gouvernementales en la matière.

3. Contexte

Le Sous-secrétariat du dirigeant principal de l'information (SSDPI) a entrepris une démarche d'architecture d'entreprise gouvernementale, y compris de l'architecture gouvernementale de l'ASIG, qui vise, d'une part, à assurer la protection des informations gouvernementales, dont les renseignements personnels, et le maintien de la confiance des citoyens à l'égard de l'État. D'autre part, cette démarche vise à soutenir la mise en place des grandes orientations gouvernementales dans le respect du cadre légal et réglementaire en vigueur au Québec. Les documents de l'ASIG ont pour finalité de fournir les fondations nécessaires aux organismes publics pour sécuriser et protéger les informations qu'ils détiennent.

Comme le gouvernement a choisi de favoriser l'utilisation des technologies de l'information tout en assurant l'optimisation des ressources en RI pour offrir de meilleurs services aux citoyens et aux entreprises à un coût raisonnable, il est primordial de revoir les façons de faire de l'État. Le virage vers la transformation de l'appareil gouvernemental est déjà amorcé et constitue certainement le facteur le plus déterminant dans l'élaboration d'une architecture d'entreprise gouvernementale. La mise au point harmonieuse de ce plan gouvernemental, dans le respect des contraintes budgétaires, nécessite la mise en œuvre d'un cadre intégrateur.

Ses principales caractéristiques sont énoncées ci-dessous.

Le nouveau cadre de gestion en RI : l'établissement de lignes directrices soutenant son élaboration s'harmonise complètement avec la volonté du gouvernement de renforcer la gouvernance des ressources informationnelles.

Le nouveau cadre de gestion en sécurité : ce nouveau cadre vise à assurer la sécurité de l'information et, ainsi, à maintenir et à rehausser la confiance des citoyens et des entreprises à l'égard de l'État et des

services publics. En outre, la sécurité de l'information figure parmi les éléments clés pour assurer la pérennité du patrimoine informationnel gouvernemental, numérique ou pas.

La vision d'affaires de l'AEG : la vision de l'AEG est un concept visant à fournir aux différents OP une direction stratégique dans le but d'offrir, à l'avenir, des services selon différents modes et canaux de nature à favoriser l'interaction et la collaboration afin de faciliter la vie des individus et des entreprises. Dans ce contexte, la mise en place de la vision nécessite des transformations profondes dans les processus de gestion et dans les méthodes de travail ainsi que dans les applications et les infrastructures.

La concrétisation de la vision : la transformation profonde des façons de faire de l'État doit s'accompagner d'une identification et d'une prise en charge des effets qu'elle entraînera sur les ressources humaines et sur les autres aspects de l'organisation. Ainsi, le passage d'une pratique de multiservices à un seul service, de procédures fermées à une interrelation organisationnelle, de données cloisonnées par organisation à des données partagées (fédérées), de traitements locaux à des traitements « interconnectés », de l'utilisation d'infrastructures propriétaires au partage d'infrastructures et de l'investissement à la consommation de ressources en informatique sont autant de façons d'aborder le dossier dans le but évident de concrétiser la vision de l'AEG.

L'accent sur les composantes communes, partageables et réutilisables : il existe un ensemble de projets d'investissement porteurs qui sont en cours d'élaboration ou de réalisation à l'échelle gouvernementale. Il faut pouvoir déterminer 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 maîtrise des coûts : bien que l'évolution des dépenses soit maîtrisée, minimiser les coûts demeure une variable importante. Le gouvernement québécois veut atteindre le déficit zéro. Comme les dépenses du gouvernement en RI représentent une part importante du budget des programmes, leur maîtrise est prioritaire.

L'angle du service aux individus et aux entreprises : les organismes publics, comme toutes les grandes organisations, changent leurs façons d'offrir les services. On se dirige vers la création de réseaux intégrés de services, la mise au point d'approches par programmes 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 pour simplifier et rendre plus transparent l'accès aux informations et aux services du gouvernement.

La force de la convergence des technologies : l'évolution rapide des technologies de l'information et des télécommunications a permis le dossier citoyen informatisé, différents dépôts de données, l'intégration des données en fonction de résultats, le télétraitement, l'inforoute de la géomatique, etc. Elle permet aux organismes publics d'envisager d'autres changements en ce qui a trait au traitement de l'information, comme le partage d'infrastructures, la mise en place de services communs, le recours à l'infonuagique, etc. L'utilisation de ces diverses technologies facilitera l'établissement de liens plus étroits et plus intégrés entre les OP tant sur le plan de leur mission que sur le plan administratif, et ce, tant à l'échelle locale qu'à l'échelle régionale ou nationale. Enfin, elles permettront de mieux évaluer la pertinence, l'efficacité et l'efficience des services offerts aux individus et entreprises.

La sécurité et la protection de l'information : l'État est amené à colliger des renseignements personnels et confidentiels sur les individus et sur les entreprises pour l'administration de ses nombreux programmes. Ces particularités posent de grands défis à l'État en matière de déploiement technologique. Renforcer la confiance à l'égard des échanges électroniques gouvernementaux est primordial.

Dans cette vision de l'État, le cadre intégrateur de la démarche de l'architecture d'entreprise gouvernementale doit impérativement faire en sorte que les principes de sécurité et de protection des renseignements personnels sont impérativement préservés. En effet, la structuration et la gestion de l'information doivent être réalisées en toute sécurité, dans le respect des lois et des règlements, tout en assurant le plus de services possible 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 document s'inscrit dans le contexte de la mise en place du nouveau cadre de gestion en RI et en sécurité ainsi que de la continuité des travaux sur l'AEG. Il vient en préciser le segment sécurité.

4. Vision et orientations

La mission de la sécurisation de l'information au gouvernement du Québec consiste essentiellement à assurer la disponibilité, l'intégrité et la confidentialité de l'information gouvernementale tout au long de son cycle de vie, et ce, à un niveau de risque résiduel considéré comme étant acceptable par l'État québécois, par ses usagers et, de manière générale, par la communauté gouvernementale. Elle doit être réalisée à un coût acceptable et proportionnel à la valeur de l'information.

Mais pourquoi l'État doit-il sécuriser ses informations? Qu'est-ce qui justifie que le gouvernement du Québec et les OP déploient des efforts parfois importants et coûteux pour protéger leurs informations? À ce stade, il apparaît important de comprendre les motivations profondes qui amènent l'État québécois à se préoccuper autant de la sécurisation des informations qu'il détient. La compréhension des raisons pour lesquelles on souhaite sécuriser est essentielle pour appuyer par la suite notre capacité à saisir et à évaluer la pertinence de l'architecture gouvernementale proposée.

Au fil du temps, une information de qualité est devenue une condition essentielle, voire critique, du succès de toute organisation. Les organisations publiques et privées sont désormais conscientes du fait qu'elles doivent disposer d'une information disponible, intègre et confidentielle pour assurer la qualité, l'efficacité et l'efficience de leur prestation de services et de leurs activités internes et, pour établir et maintenir le lien de confiance indispensable qui les unit à leur clientèle et à leurs partenaires.

Une information mal protégée engendre des conséquences néfastes majeures pour toute organisation. En effet, en l'absence d'une protection appropriée, une organisation s'expose à des risques réels non maîtrisés en ce qui concerne l'information qu'elle détient, des risques pouvant engendrer une cascade d'effets potentiels négatifs inacceptables pour l'organisation, pour ses partenaires ou pour sa clientèle.

Ainsi, une organisation qui ne protège pas adéquatement ses informations s'expose considérablement au risque de faire l'objet de fraudes, d'erreurs, de bris, de failles ou de malveillance en ce qui concerne ses informations. Le cas échéant, l'occurrence d'une de ces situations peut engendrer une perte de disponibilité, d'intégrité ou de confidentialité des informations, une perte de sécurité qui peut se traduire, pour cette organisation, par un ensemble de conséquences négatives et importantes pour les citoyens et les entreprises, par exemple, la divulgation d'informations sensibles, une perte d'efficacité, d'efficience et de qualité de la prestation des services ou une perturbation de ses activités internes, des pertes financières ou matérielles, des restrictions importantes quant à l'utilisation du potentiel d'affaires et, plus important encore, une perte de confiance et une baisse de la satisfaction des clientèles.

Devant la valeur stratégique de leurs informations ainsi que la nature et l'envergure des impacts potentiels « inacceptables » découlant d'une information mal sécurisée, l'État québécois et la communauté gouvernementale en général sont conscients que leurs informations doivent être suffisamment protégées pour que les risques auxquels elles sont exposées soient maintenus à un niveau acceptable.

Loin d'être considérés comme une dépense, les efforts nécessaires pour sécuriser les informations de l'État doivent être compris comme un investissement stratégique, une occasion d'affaires, voire un catalyseur visant à fournir les garanties préalables de qualité et de stabilité de l'information gouvernementale indispensables au bon fonctionnement et à l'évolution des activités de l'État québécois, ainsi qu'au maintien d'un lien de confiance solide avec ses usagers.

L'approche de développement de l'architecture prend en compte une vision globale de la sécurité axée sur un encadrement juridique, humain, organisationnel (processus) et technologique favorisant la protection des informations et des infrastructures gouvernementales. Aujourd'hui, il est essentiel de récupérer au maximum les acquis organisationnels tout en exploitant les nouvelles avenues offertes par

les technologies de l'information et des communications et en assurant la protection des informations gouvernementales.

Ainsi, à la nouvelle prestation électronique de services (PES) multicanaux et multimodes protégée s'ajoutent le partage de services et d'environnements informatiques, la mise en place d'infrastructures orientées service et l'ouverture à l'infonuagique, qui deviennent le fer de lance de l'architecture d'entreprise gouvernementale. À cette fin, l'ASIG doit privilégier une architecture ouverte et flexible afin de favoriser l'utilisation des nouveaux modes d'acquisition des services, l'interopérabilité des services et des échanges d'informations protégés, tout en assurant la sécurité des environnements et en respectant la protection de la vie privée par des mesures et par des mécanismes de sécurité appropriés.

Par contre, cette transformation gouvernementale « services en réseau : partagés, communs ou acquis » engendre de nouveaux risques pour la sécurité des informations gouvernementales, notamment des risques associés à une prestation gouvernementale faisant intervenir plusieurs parties prenantes, des risques associés à la prise en charge adéquate des menaces et des incidents de sécurité à l'échelle gouvernementale ainsi que des risques accrus entourant l'utilisation d'une identification gouvernementale unique pour accéder à l'ensemble des services de l'État.

L'architecture de sécurité de l'information devra démontrer clairement sa contribution à la transformation de l'État en ce qui a trait à l'amélioration de la satisfaction de la clientèle ainsi qu'à l'efficacité, à l'efficience et à l'agilité de l'appareil gouvernemental. Plus important encore, elle devra s'assurer d'avoir la capacité de protéger les informations de la nouvelle prestation gouvernementale « en réseau : services partagés, communs ou acquis » contre les nouveaux risques de sécurité de l'information, au fur et à mesure que celle-ci sera déployée dans l'administration publique québécoise.

Dans un dossier aussi complexe et nécessaire que celui de l'architecture d'entreprise gouvernementale, la sécurité doit prendre en considération les différentes interactions qui existent entre les clientèles et les OP ainsi qu'entre les OP pour le partage des services, des infrastructures ou des échanges d'informations protégés.

C'est ici que la vision de la sécurité d'entreprise prend tout son sens. Les énoncés de vision et des orientations viennent préciser un certain nombre d'éléments structurants pris en compte dans le présent document pour guider l'élaboration de l'ASIG de l'architecture d'entreprise gouvernementale. En effet, la sécurité doit être perçue comme un moyen de faciliter l'accès sécuritaire à l'information, de permettre des échanges électroniques sécurisés en toute confiance et d'assurer la protection de l'environnement gouvernemental.

Cette vision est étroitement liée aux pratiques et aux lignes directrices du nouveau cadre de gouvernance en sécurité de l'information du gouvernement du Québec. Ainsi, l'ASIG doit :

- ✓ Diffuser une vision commune des principales composantes de la sécurité, associée étroitement 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 cible de la sécurité de l'information gouvernementale.

Vision : Assurer un environnement gouvernemental sécurisé et digne de confiance

Sept énoncés d'orientation sont proposés et regroupés selon deux points de vue : celui de l'usager et celui de l'administration gouvernementale.

Du point de vue de l'administration gouvernementale :

- ✓ **Orientation 1 :** Respecter le cadre législatif et réglementaire (conformité).
- ✓ **Orientation 2 :** Assurer la protection adéquate de l'information du gouvernement du Québec.
- ✓ **Orientation 3 :** Simplifier le discours d'affaires sur la sécurité de l'information gouvernementale.
- ✓ **Orientation 4 :** Prendre en compte le nouveau cadre de gestion en RI afin de favoriser la cohérence des actions en sécurité à l'échelle tant gouvernementale que sectorielle.

- ✓ **Orientation 5 :** Sécuriser l'information de la nouvelle prestation de services gouvernementaux commune et en réseau en émergence au gouvernement du Québec.

Du point de vue de l'usager gouvernemental :

- ✓ **Orientation 6 :** Contribuer à la consolidation et au maintien du lien de confiance qui unit l'usager gouvernemental et l'État québécois.
- ✓ **Orientation 7 :** Satisfaire les attentes des usagers gouvernementaux en matière de sécurité de leurs informations.

Ces grandes orientations visent à :

- ✓ Encadrer les façons de faire en matière de sécurité de l'information;
- ✓ Respecter le contexte d'affaires des organismes publics et leurs besoins;
- ✓ Influer sur les architectures d'entreprise gouvernementale et sectorielle.

Toute solution gouvernementale en sécurité de l'information devra s'assurer de satisfaire aux énoncés présentés ci-dessous.

Orientation 1 : Respecter le cadre législatif et réglementaire (conformité)

La conformité des informations gouvernementales s'appuie sur le respect du cadre juridique et réglementaire « global » entourant toute activité de l'État québécois et, plus particulièrement, sur le respect des éléments qui ont une influence directe sur l'application de la sécurité de l'information au gouvernement du Québec.

Les lois et les règlements ayant le plus d'incidence sur la sécurité sont présentés ci-dessous. Ainsi, sans en faire une liste exhaustive, il sera nécessaire de considérer les éléments légaux suivants:

- ✓ Les lois Québécoises ayant une incidence majeure sur la sécurité de l'information, notamment :
  - « La Loi sur l'administration publique »;
  - « La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement »;
  - « la Loi concernant le cadre juridique des technologies de l'information »;
  - « La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et la Loi la modifiant (2006) »;
  - « La Loi sur la protection des renseignements personnels dans le secteur privé »;
  - « La Loi sur les archives nationales »;
  - « Le Code civil ».
- ✓ Les lois canadiennes qui s'appliquent ou qui sont susceptibles de s'appliquer au Québec en matière de sécurité de l'information, notamment :
  - « La Loi sur la protection des renseignements personnels et les documents électroniques »;
  - « La Loi sur les droits d'auteur »;
  - « la Loi sur la propriété intellectuelle et les marques de commerce »;
  - « La Charte des droits et libertés de la personne ».
- ✓ Auxquelles il faut ajouter :
  - Les lois québécoises sectorielles;
  - Les contrats, ententes et conventions;
  - Autres considérations d'ordre juridique.

Orientation 2 : Assurer la protection adéquate de l'information du gouvernement du Québec

La disponibilité, l'intégrité et la confidentialité de l'ensemble des informations gouvernementales doivent être assurées à la grandeur du gouvernement du Québec, et ce :

- ✓ Que ces informations soient utilisées pour la prestation de services ou pour la gestion interne;
- ✓ Quel que soit le support de l'information ou le canal ou le mode d'accès utilisé;
- ✓ Quelle que soit l'organisation publique ou privée concernée;
- ✓ Que ces informations soient conservées dans un dépôt ou en circulation dans ses échanges internes ou externes;
- ✓ Tout au long de leur cycle vie.

Orientation 3 : Simplifier le discours d'affaires de la sécurité de l'information gouvernementale

À ce jour, la volonté d'appropriation de la sécurité de l'information par les décideurs gouvernementaux se bute couramment à un discours hermétique et technique du domaine de la sécurité de l'information. C'est pourquoi un discours d'affaires simplifié en matière de protection des informations doit être adopté de manière à ce qu'il soit adapté aux préoccupations d'affaires des décideurs et des usagers de l'État québécois.

Les plans d'affaires de la solution gouvernementale de SI qui leur sont destinés doivent leur permettre de comprendre rapidement la raison pour laquelle ils doivent sécuriser leurs informations et la façon de procéder pour y arriver à coûts raisonnables. Ces plans doivent être épurés des termes techniques et être faciles à comprendre et à communiquer.

Orientation 4 : Prendre en compte le nouveau cadre de gestion en RI afin de favoriser la cohérence des actions en sécurité à l'échelle tant gouvernementale que sectorielle

La gouvernance et la gestion des ressources informationnelles au sein de l'État soulèvent des enjeux majeurs pour les citoyens, les entreprises, les organismes et l'administration publique. En fait, ces enjeux touchent l'ensemble de la société québécoise.

Un des objectifs de la politique cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics consiste à assurer la sécurité de l'information et, ainsi, à maintenir et à rehausser la confiance des citoyens et des entreprises à l'égard de l'État et des services publics. En outre, la sécurité de l'information figure parmi les éléments clés de la pérennité du patrimoine informationnel gouvernemental.

Le dirigeant principal de l'information (DPI) a formalisé, au moyen de plusieurs documents structurants, les éléments visant à instaurer une gouvernance forte et intégrée de la sécurité de l'information et à concrétiser la vision gouvernementale en la matière. Le gouvernement du Québec confirme ainsi que la sécurité de l'information est une priorité. L'utilisation sans cesse accrue d'informations de toutes natures concernant les citoyens, les entreprises et les organismes publics soulève des questions cruciales, soit celles de la disponibilité de l'information, de son intégrité et de sa confidentialité.

L'établissement d'une gouvernance en sécurité de l'information doit :

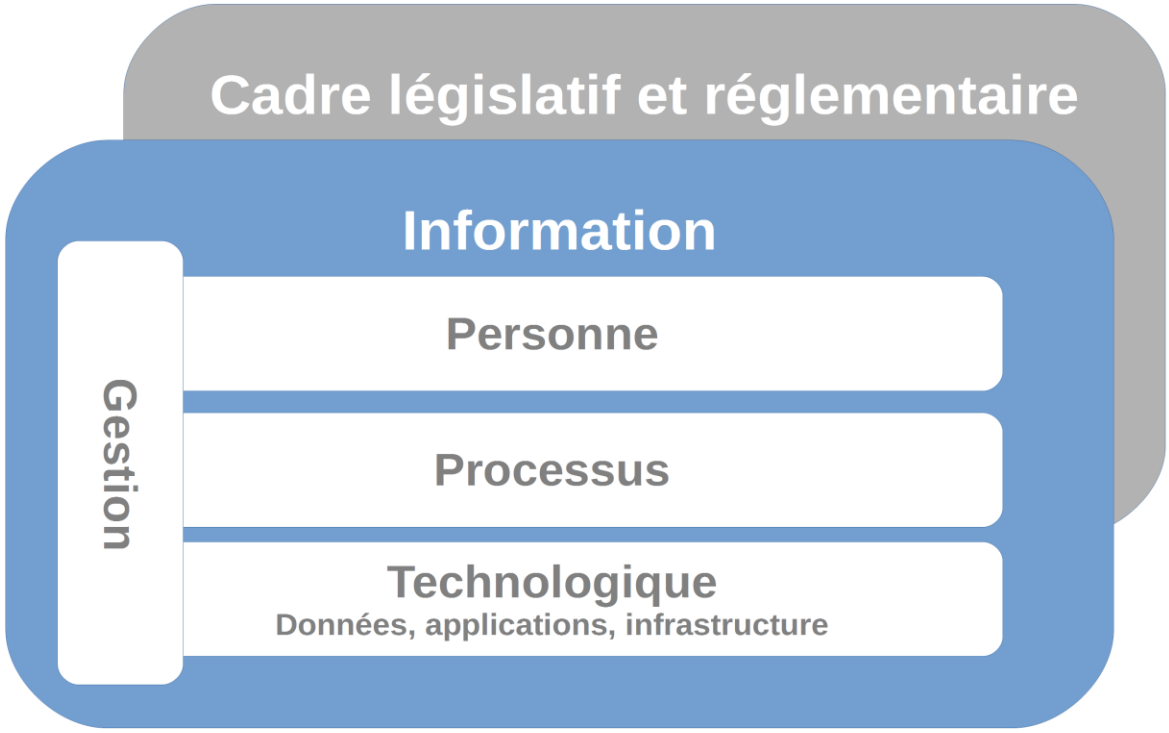
- ✓ Fournir une approche cohérente, intégrée et alignée sur l'approche de la gouvernance de l'organisation. Cette cohérence permet de s'assurer que les décisions sont prises en accord avec les stratégies et les objectifs de l'organisation, que les processus sont suivis de manière efficace et transparente, conformément aux dispositions légales et réglementaires, et que les responsabilités des intervenants en matière de sécurité sont remplies.
- ✓ Assurer une valeur optimale des investissements en matière de sécurité permettant d'offrir une prestation sécuritaire, économique et fiable de services, d'établir un portait précis des coûts et

des avantages probables, de telle sorte que les besoins de l'organisation soient pris en charge de manière efficace et efficiente.

- ✓ Assurer que les risques soient évalués adéquatement selon des seuils de tolérance établis, que les effets de ces risques soient prévus et gérés de manière appropriée, et que les risques de non-conformité soient réduits au minimum.
- ✓ Veiller à ce que les besoins en ressources de l'organisation soient comblés de manière optimale, que les coûts soient optimisés, que les conditions soient en place afin de maximiser la probabilité de succès des projets en cours et à venir.
- ✓ Assurer une communication efficace et en temps opportun aux parties prenantes en matière de sécurité, fournir des indicateurs pour accroître les performances, cibler les domaines d'amélioration et confirmer que les objectifs et orientations en matière de sécurité sont en ligne avec la stratégie de l'organisation.

Une gestion intégrée de la sécurité de l'information, étroitement liée à la culture de l'organisation, repose dans un premier temps sur divers piliers de gestion, tel qu'ils sont illustrés à la figure 1.

Figure 1 : Domaines de la gestion de la sécurité



La gestion des personnes repose sur les compétences (expertises et expériences) des intervenants en matière de sécurité afin que soient prises les bonnes décisions sur les diverses mesures à mettre place. Les notions de culture, d'éthique et de comportement sont autant de facteurs de réussite dans les activités de gouvernance et de gestion. Or, elles sont souvent sous-estimées.

Les processus de gouvernance, de gestion ou opérationnels, se compose d'un ensemble organisé de pratiques et d'activités formellement documentées. Son objectif consiste à atteindre certains objectifs liés à la sécurité de l'information.

La gestion des services inclut les applications et les infrastructures technologiques qui fournissent les moyens informatiques d'implémenter les services de sécurité de l'information.

Par ailleurs, la gestion intégrée de la sécurité dans une organisation passe par une gestion intégrée du risque (gouvernance, gestion du risque et conformité). Cette approche permet d'éviter les principaux pièges lorsque chacun des éléments de la gestion intégrée de la sécurité est considéré en silo.

Notons également que le cadre de référence COBIT 5, dans son approche intégrée de gestion de la sécurité, considère quant à lui plusieurs composantes du modèle d'affaires de la sécurité de l'information. Ces composantes sont intégrées en tant que facilitateurs afin de soutenir l'organisation dans l'atteinte de ses objectifs et, ainsi, de créer une valeur ajoutée pour les parties prenantes. On y retrouve :

- ✓ Des activités associées à la gouvernance dans plusieurs processus;
- ✓ Un processus de gestion des risques et des orientations pour les faciliter;
- ✓ Une importance particulière accordée aux activités de conformité.

Ainsi, par la mise en place d'une gestion intégrée du risque, une organisation peut démontrer un niveau de maturité supérieur dans la prise en charge globale de la sécurité de l'information. Il convient donc à un organisme public de concrétiser cette mise en place en se dotant d'un modèle d'établissement, de mise en œuvre, de fonctionnement, de surveillance, de réexamen, de mise à jour et d'amélioration d'un système de gestion de la sécurité de l'information (SGSI). La conception et la mise en œuvre du SGSI d'un organisme tiennent compte des besoins et des objectifs, des exigences de sécurité, des mesures de sécurité, des processus suivis, ainsi que de la taille et de la structure de l'organisme.

L'architecture de sécurité de l'information à l'échelle de l'entreprise soutient la mise en œuvre de la sécurité de l'information en déterminant et en organisant, dans un ensemble cohérent, les éléments architecturaux qui lui sont nécessaires. Dans ce contexte, l'établissement de lignes directrices soutenant son élaboration s'harmonise complètement avec la volonté du gouvernement de renforcer la gouvernance des ressources informationnelles exprimée clairement par l'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement[4]. De plus, le cadre de gouvernance en sécurité de l'information découle principalement de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. Le cadre de gouvernance en sécurité de l'information issu de cette loi définit par ailleurs les rôles nécessaires à l'élaboration de l'architecture de sécurité de l'information (ASI).

L'ASI est une pièce maîtresse de la planification des actions en sécurité d'une organisation (programme de sécurité). Elle sert à communiquer de manière cohérente ses différents constituants dans l'organisation. Elle est conçue itérativement, sous la forme d'une collection de documents, et fait le lien entre les objectifs d'affaires de l'organisation et un ensemble de solutions qui lui sont propres.

Comme l'ASI doit refléter le fin maillage entre la sécurité et l'organisation, elle est mise au point, idéalement, en tant que segment de l'architecture d'entreprise. Cependant, cela n'est possible que pour des organisations qui disposent à la fois d'une architecture d'entreprise mature et qui présentent une excellente collaboration entre les responsables de l'architecture d'entreprise et les responsables de la sécurité.

En revanche, en raison de son importance dans le soutien du programme de sécurité et dans la saine gestion de la sécurité, l'ASI demeure impérative, même si elle est mise au point seule. Elle doit alors tenir compte de l'environnement de l'organisation à chaque nouvelle itération, pour chacune de ses composantes.

4. Secrétariat du Conseil du trésor, Pratique recommandée : Modèle de référence en architecture de la sécurité de l'information (document de travail), décembre 2014.

Orientation 5 : Sécuriser l'information de la nouvelle prestation de services gouvernementaux commune et en réseau en émergence au gouvernement du Québec.

Les objectifs gouvernementaux de transformation visent à créer un État qui se démarque par la qualité, l'accessibilité et la simplification des services qu'il offre à ses clientèles, par l'utilisation optimale de ses ressources, notamment en privilégiant une contribution significative des ressources informationnelles, et par une gestion des résultats.

À terme, cet État « transformé » devrait se traduire par un accroissement notable de la satisfaction de la clientèle et par un gain substantiel d'efficacité, d'efficience et d'agilité de l'ensemble des activités gouvernementales. Plus important encore, la modernisation de l'État devrait se traduire par l'émergence progressive d'une nouvelle prestation gouvernementale de services organisée « en réseau » en fonction des attentes des clientèles, laquelle est caractérisée notamment par le modèle et les éléments de vision suivants, extraits des principes généraux de la prochaine version de l'architecture d'entreprise gouvernementale.

Dans cette nouvelle prestation, l'État québécois évolue pas à pas de la prestation « ministérielle », traditionnellement en « silo », vers une prestation « gouvernementale » en réseau caractérisée par :

L'usager au centre de la prestation de services gouvernementale, qui se traduit par une écoute constante des attentes des usagers, un niveau de service garanti publiquement, une offre de services gouvernementale organisée en fonction des besoins ou des événements de la vie des usagers et, possiblement, enrichie par les services d'autres juridictions ou ceux d'organisations privées, le libre choix du mode de prestation, une expérience de prestation de qualité, simplifiée, cohérente, équitable.

Le gouvernement du Québec organisé comme une « organisation unique » à l'intérieur de laquelle un usager utilise une identification potentiellement unique pour accéder, par des guichets gouvernementaux, à une offre de services globale faisant intervenir en réseau plusieurs organisations et partenaires gouvernementaux.

La nouvelle prestation est normalisée et interopérable à l'échelle gouvernementale. Elle est soutenue par le dossier client gouvernemental et ministériel intégré. Elle fait l'objet d'un engagement gouvernemental sur la qualité de la prestation, d'une gestion gouvernementale de la relation clientèle, d'une gouvernance accrue.

Une « pensée globale », c'est-à-dire une action gouvernementale et ministérielle cohérente qui souligne la volonté d'agir tous ensemble vers une cible gouvernementale commune en se basant notamment sur :

- ✓ La mise en place d'une culture et d'une vision communes de la prestation cible ainsi que sur une coordination gouvernementale renforcée, notamment en ce qui a trait à l'arrimage des opérations et des projets d'évolution de l'État;
- ✓ La priorité au partage et à la réutilisation de solutions administratives et techniques communes partout où c'est possible et des solutions équivalentes pour le reste;
- ✓ L'importance stratégique de l'information basée sur l'identification et la réutilisation à l'échelle gouvernementale de « sources officielles d'information ».

L'alignement stratégique des ressources informationnelles sur la cible d'affaires de l'État, ce qui sous-entend des solutions de RI conçues, au premier chef, pour satisfaire les exigences de la prestation gouvernementale, ainsi que la réutilisation prioritaire de ces solutions par les autres activités de l'État québécois.

Le maintien du « lien de confiance » entre les usagers et l'État québécois est basé sur la protection adéquate de l'ensemble des informations gouvernementales. La sécurisation de ces informations constitue une des conditions essentielles au succès de cette démarche de transformation en profondeur de l'administration publique québécoise.

Orientation 6 : Contribuer à la consolidation et au maintien du lien de confiance qui unit l'usager et l'État québécois

De façon très générale, le concept de confiance est une « attitude positive dans l'absence de garantie ». Ce concept très abstrait est étroitement lié à la présence de menaces qui exploitent une vulnérabilité et des conséquences de la matérialisation d'un risque lors d'un événement (risque). En effet, en l'absence d'un risque encouru, on ne peut parler de confiance à l'égard d'autrui. La confiance est importante en ce qu'elle constitue un pont entre l'incertitude et l'action. Ainsi, dans un environnement où l'on manque de certitude par rapport aux résultats escomptés, la confiance allège les procédures autrement complexes et introduit un climat sain qui encourage et favorise le partage ou les échanges.

Dans le domaine de la prestation de services de l'administration publique, la confiance peut se définir comme le « sentiment que l'autre partie de l'échange (individu, groupe, organisation) agira avec honnêteté et qu'elle dispose de la compétence nécessaire pour accomplir la prestation attendue ». La sécurité de l'information et des échanges constitue un des facteurs prépondérants dans l'établissement de la relation de confiance. D'autres facteurs favorisent aussi le maintien et le rehaussement de la confiance, notamment :

- ✓ La réputation et la crédibilité liées à la renommée et à l'image qui peuvent être établies notamment par un sceau de certification ou des affiliations;
- ✓ Une expérience positive avec l'organisation, notamment dans sa capacité de satisfaire les attentes des usagers, dans une rétroaction en temps réel et par l'absence de conséquences inattendues ou non mentionnées.

La qualité du service reçu, notamment au regard de la facilité d'utilisation, de la qualité des informations et de l'uniformité de service, repose sur :

- ✓ La gestion de la relation avec les usagers;
- ✓ La protection des renseignements personnels et le respect de la vie privée;
- ✓ L'équilibre entre le respect de la vie privée et l'efficacité du service;
- ✓ Un cadre légal bien défini;
- ✓ La transparence des procédures et des échanges, notamment en cas d'incident;
- ✓ Une adaptabilité de l'offre aux réalités sociales, linguistiques et individuelles du public.

Toute approche ou solution en sécurité de l'information gouvernementale doit donc contribuer solidement à ce que l'État québécois soit considéré comme étant digne de confiance par l'usager L'organisation et les solutions de sécurité gouvernementales mises en place doivent permettre à l'ensemble des usagers gouvernementaux de susciter la conviction que leurs informations sont bien protégées afin d'en assurer la disponibilité, l'intégrité et, surtout, la confidentialité, et ce, à un niveau de confiance correspondant à leurs attentes. Cela est particulièrement vrai en ce qui concerne la protection de leurs informations d'identification et l'accès à leurs informations critiques.

Orientation 7 : Satisfaire les attentes des usagers en matière de sécurité de leurs informations

Ainsi, en matière de sécurisation de ses informations, l'usager doit être convaincu que l'État québécois a fait ses devoirs et qu'il continue à les faire. Ce message gouvernemental de confiance doit être clair, sans équivoque et pouvoir être démontré en tout temps par la mise en place des moyens suffisants.

La satisfaction de la clientèle est désormais au centre des préoccupations de la prestation de services actuelle et en devenir de l'État québécois. Cette orientation fondamentale de service orienté client oblige l'ensemble des intervenants publics ou privés participant à la prestation gouvernementale de services à s'assurer que les attentes des usagers sont connues, comprises et prises en charge.

Cette obligation est encore plus marquante en matière de sécurisation des informations gouvernementales, car la satisfaction des attentes des usagers gouvernementaux en matière de sécurité

de l'information (SI) constitue une pierre d'assise à l'établissement et au maintien du lien de confiance qui les unit à l'État québécois.

5. Principes généraux de sécurité

La technologie a changé la façon dont les affaires ou les activités sont menées dans les organisations. La gestion de l'information est désormais au cœur de la gouvernance des organisations. L'utilisation accrue de nouveaux modes d'acquisition des ressources en TI, de la connectivité et de l'Internet pour les services présente des risques pour les organisations. Ces risques doivent être gérés avec soin par la création et la mise en œuvre des politiques appropriées, des processus et des technologies.

Afin de s'adapter à ces exigences complexes, les organisations ont besoin de réexaminer la manière dont les actifs informationnels de l'organisme sont organisés et gérés. Cela a conduit à l'adoption plus large de stratégies telles que la modélisation des stratégies d'affaires dans le cadre de l'élaboration d'architectures d'entreprise.

Le défi pour les organisations est de mettre en place une architecture de services flexible tout en maintenant un niveau de sécurité adéquat. Les organisations doivent examiner attentivement, en plus de la fiabilité, la confidentialité, l'intégrité et la disponibilité de l'information qu'ils traitent ou utilisent. Ainsi, compte tenu de l'évolution actuelle des environnements technologiques, il est nécessaire de remettre l'accent sur les principes de base en sécurité et de les recadrer, tel qu'ils s'appliquent à une architecture d'entreprise.

Cette section propose sept principes de base de la sécurité de l'information qui fournissent un ensemble d'exigences essentielles à prendre en considération afin d'assurer que la sécurité de l'information est traitée par une architecture d'entreprise dans le contexte de la mise en place d'une gouvernance forte de la sécurité. Les principes généraux de sécurité de l'information mis en avant découlent d'un travail d'analyse d'un certain nombre de principes existants proposés par des organismes de normalisation en sécurité reconnus internationalement. Ces principes et les recommandations pratiques qui les accompagnent sont en accord avec les quatre principes directeurs de la directive de sécurité de l'information.

L'alignement de l'architecture d'entreprise sur les exigences de sécurité de l'information peut être obtenu par la mise en application des principes énoncés dans le présent document. De plus, le recours à ces principes généraux peut faire en sorte que l'architecture de sécurité demeure actuelle, mesurable et apte à protéger adéquatement l'information gouvernementale.

Ces principes ne sont pas nouveaux; ils sont destinés à être intemporels :

Principe 1 : La sécurité de l'information fait partie intégrante de la stratégie d'affaires de l'organisation.

Principe 2 : La sécurité de l'information a des effets sur l'ensemble de l'organisation.

Principe 3 : La gestion des risques détermine les exigences de sécurité.

Principe 4 : Les responsabilités en sécurité de l'information sont définies et attribuées.

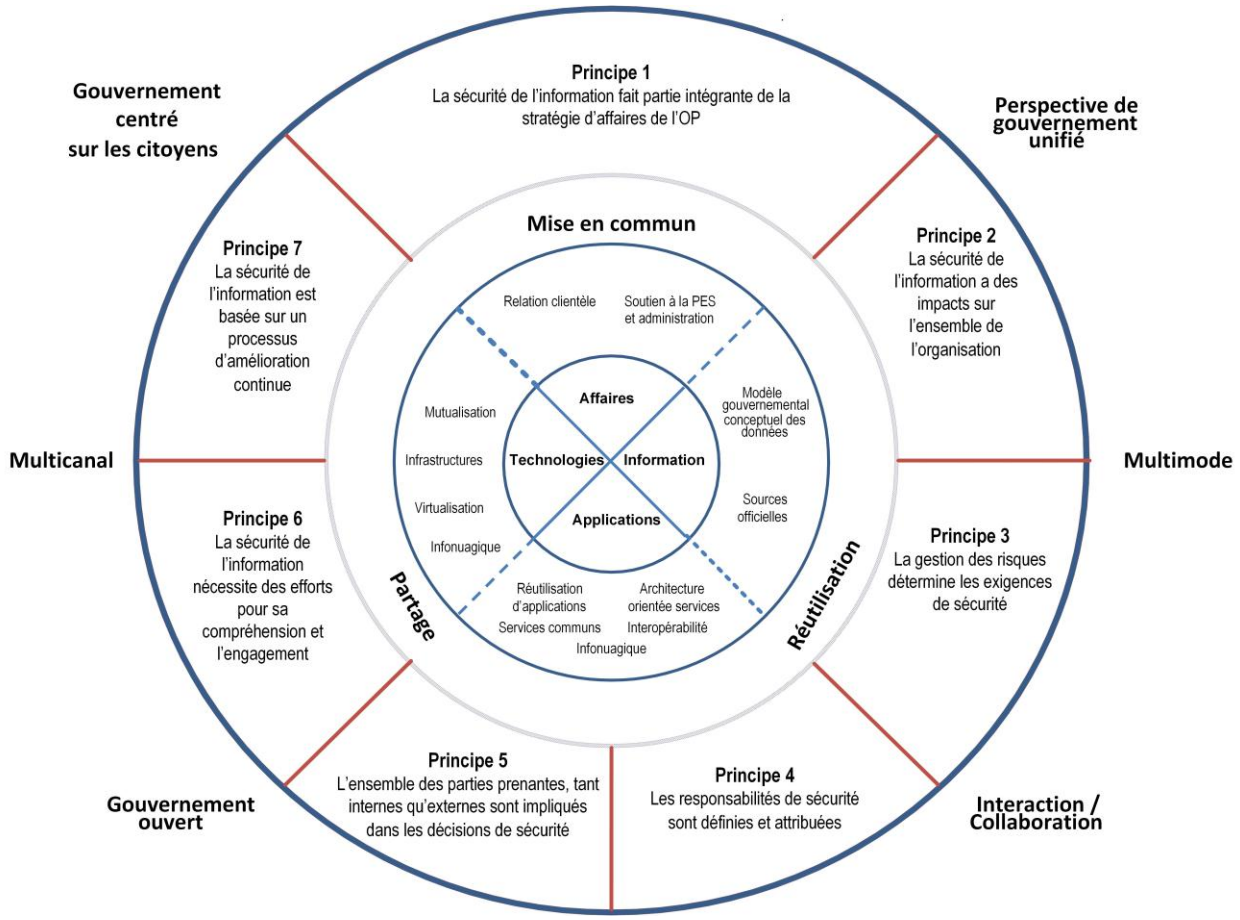
Principe 5 : L'ensemble des besoins en sécurité des parties prenantes, tant internes qu'externes, est pris en compte.

Principe 6 : La sécurité de l'information nécessite des efforts pour sa compréhension et pour favoriser l'engagement.

Principe 7 : La sécurité de l'information est basée sur un processus d'amélioration continue.

La figure 2 résume la relation entre ces principes et les éléments de l'architecture d'entreprise. Les principes, distribués sur un anneau extérieur, sont utilisés pour définir et concevoir l'architecture d'entreprise, dont les composantes sont spécifiées sur l'anneau intérieur, et pour assurer l'intégration dans les composantes d'architecture d'entreprise et entre elles.

Figure 2 : Relation entre les principes généraux de sécurité et l'architecture d'entreprise



5.1 Présentation des principes généraux en sécurité de l'information

Ces principes ont aussi été établis pour guider la mise en œuvre de la sécurité de l'information dans les OP. Ces derniers peuvent les utiliser pour planifier et mettre au point la sécurité de leur environnement et, ainsi, assurer la protection de leurs actifs informationnels ou ceux qu'ils détiennent à titre de tiers. L'ensemble des principes établis est destiné à fournir un cadre de bonnes pratiques qui permettra aux OP d'adopter les stratégies, les mesures et les technologies de sécurité éprouvées. En particulier, la compréhension des principes et leur intégration dans le cycle de gestion de l'organisation sont des aspects essentiels du système de gestion de la sécurité de l'information.

Ces principes sont pertinents à l'ensemble des OP pour la conception, la mise au point et l'évolution d'une stratégie afin d'améliorer la sécurité lors de la réalisation de projets de mise à niveau de la sécurité ou de favoriser la prise en compte des enjeux et des exigences lors de la réalisation d'une architecture de sécurité de niveau entreprise. L'application de ces principes permettra de protéger les actifs informationnels des organismes dans l'environnement changeant d'aujourd'hui, un objectif clé de gouvernance de la sécurité de l'information.

Ces principes sont également destinés à permettre aux OP de mieux répondre à leurs obligations quant à la gouvernance de la sécurité de l'information de leur organisation, y compris en ce qui a trait à la conformité légale et réglementaire. Les principes de sécurité de l'information dans l'architecture d'entreprise permettent à l'organisation d'appliquer et de mettre en place les meilleures mesures et

procédures pratiques pour satisfaire l'esprit et la lettre de presque tout cadre de normalisation en sécurité de l'information. L'utilisation de cadres de normalisation reconnus internationalement (tel qu'ISO 27001) lors de la mise au point d'un programme de sécurité de l'information permettra de fournir les bases pour la construction d'une réponse adéquate aux exigences législatives et réglementaires.

Finalement, grâce à l'intégration de ces principes par les OP dans leurs activités quotidiennes, que ce soit par la planification de la direction stratégique de l'organisation ou tout simplement dans la gestion courante des opérations quotidiennes, une « culture de sécurité » s'installera. Elle appuiera les efforts de protection continue des actifs informationnels de l'organisation et soutiendra les obligations légales et réglementaires de conformité de l'organisation.

Principe 1 : Sécurité de l'information fait partie intégrante de la stratégie d'affaires de l'organisation (OP)

La sécurité de l'information est un soutien essentiel aux objectifs d'affaires de la stratégie de l'organisation à la fois parce qu'elle minimise les risques et maintient la confiance à l'égard du déploiement des nouvelles générations de services. Dans ce contexte, la sécurité de l'information doit recevoir l'aval et être soutenue par la haute direction. Pour soutenir efficacement la stratégie d'entreprise, la sécurité de l'information nécessite l'appui de la haute direction. Le déploiement efficace de mesures de sécurité de l'information contribue à la mission des OP en :

- ✓ Protégeant les ressources informationnelles, matérielles et financières, la réputation, la situation juridique, les employés et d'autres actifs corporels et incorporels;
- ✓ Offrant des possibilités d'introduire de nouveaux services et de se connecter à des partenaires avec confiance.

La mise en œuvre de ce principe a les implications suivantes :

- ✓ Mettre au point une stratégie de sécurité de l'information cohérente avec les objectifs d'affaires et les responsabilités de l'ensemble de l'organisation; elle doit être approuvée par la haute direction;
- ✓ Intégrer la planification de la sécurité de l'information à la planification stratégique et opérationnelle et en assurer la cohérence;
- ✓ La haute direction doit manifester son soutien à la sécurité de l'information à tous les échelons de l'organisme;
- ✓ Assurer la conformité de la sécurité de l'information aux exigences légales et réglementaires.

Principe 2 : La sécurité de l'information a une influence sur l'organisation entière (OP)

Une approche globale dans la mise en œuvre de la sécurité de l'information est généralement reconnue comme étant la plus rentable. Il s'agit de considérer les personnes, les processus et les technologies de toutes les sphères de l'organisation. Afin de maximiser le retour sur investissement en matière de sécurité, elle doit être conçue dès le début dans les systèmes d'information et les processus. Une approche globale assure que la sécurité de l'information atteint les objectifs suivants :

- ✓ La coopération des personnes et des secteurs concernés et l'acceptation par l'organisation;
- ✓ L'implémentation de mesures de sécurité de l'information qui répondent aux besoins concrets des organisations et qui s'intègrent facilement;
- ✓ L'optimisation du ratio coût-efficacité des mesures de sécurité sélectionnées.

La mise en œuvre de ce principe a les implications suivantes :

- ✓ Impliquer toutes les parties prenantes, tant internes qu'externes, lors de la prise de décision sur des enjeux de sécurité de l'information;
- ✓ Mettre en œuvre des processus qui assurent des solutions pratiques et rapides en sécurité de l'information;

- ✓ Considérer les aspects de la sécurité physique et de la protection des personnes comme parties intégrantes de la sécurité de l'information;
- ✓ Impliquer la direction des ressources humaines dans la sécurité de l'information afin d'assurer que le personnel est géré en conformité avec les prescriptions de sécurité de l'organisme;
- ✓ Intégrer la sécurité de l'information dans le cycle de vie des systèmes d'information (cadre de développement de l'organisation);
- ✓ Mettre en œuvre des solutions de sécurité basées sur la transparence, documentées, fiables et éprouvées;
- ✓ Implémenter l'approche de sécurité par couches et assurer la sécurité des couches technologiques.

Principe 3 : La gestion des risques détermine les exigences de sécurité

Une pratique fondamentale en management est la gestion du risque. Une de ces composantes est la gestion des risques pour la sécurité de l'information. Les organismes publics doivent les évaluer, s'en protéger et faire rapport. Le traitement proposé pour la gestion des risques repose sur une approche de gestion des exigences de sécurité de l'information, dont un des postulats est que le choix des mesures doit être proportionnel aux conséquences des risques. Adopter cette approche s'accompagne des avantages suivants :

- ✓ La prise en compte par la haute direction, de l'effet de la sécurité de l'information sur l'organisation;
- ✓ La gestion du risque d'entreprise, d'être informé des besoins en matière de sécurité administrative et technique dans la gestion risque de sécurité de l'information;
- ✓ Le traitement des risques de sécurité de l'information et l'établissement de priorités en fonction des besoins opérationnels de l'organisme;
- ✓ La justification des dépenses en sécurité de l'information et la contention des dépassements de coûts possibles.

La mise en œuvre de ce principe a les implications suivantes :

- ✓ La gestion des risques de sécurité doit être intégrée au processus général de gestion des risques de l'organisme;
- ✓ Les priorités parmi les risques de sécurité doivent être établies et leur traitement doit être proportionnel aux conséquences sur l'organisation.

Principe 4 : Les responsabilités en sécurité de l'information sont définies et attribuées

Les organisations devraient élaborer et mettre en œuvre formellement le cadre gouvernemental de gestion en sécurité de l'information. Les responsabilités en sécurité peuvent également s'étendre à l'extérieur des frontières organisationnelles, notamment aux sous-traitants, à d'autres organismes publics, à des partenaires et à des mandataires. Tous les utilisateurs de systèmes d'information doivent être informés des conséquences de leurs actes.

Les responsabilités et les relations entre les personnes, les processus et les informations doivent être clairement définis, documentés et compris selon les exigences de gouvernance d'entreprise.

La mise en œuvre de ce principe a les implications suivantes :

- ✓ Rendre imputables les cadres dirigeants à l'égard de l'état de la sécurité de l'organisme;
- ✓ Attribuer les responsabilités de sécurité à tous les échelons de l'organisation;
- ✓ Allouer les responsabilités de sécurité de l'information en fonction du rôle des employés dans l'organisme;

- ✓ Définir les responsabilités en matière de sécurité pour les parties externes dans le contrat d'engagement.

Principe 5 : L'ensemble des besoins en sécurité de l'information des parties prenantes, tant internes qu'externes sont pris en compte

Comme l'interdépendance des systèmes augmente, l'importance de la sécurité de chaque composant est accrue. Les intérêts légitimes des différentes parties prenantes, ce qui comprend les partenaires, les mandataires, les fournisseurs et autres, doivent être considérés lors de la prise de décision sur des questions de sécurité de l'information. On doit être en mesure de répondre aux attentes de sécurité de l'ensemble. En considérant les attentes des différentes parties prenantes, tant internes et qu'externes, une organisation peut s'assurer qu'elle :

- ✓ Protège les intérêts des partenaires (y compris ceux des utilisateurs finaux en amont);
- ✓ Assure la cohérence dans la protection des données tout au long de la chaîne d'approvisionnement des différents partenaires concernés par la livraison d'un produit ou d'un service;
- ✓ Assure le maintien de la confiance entre l'organisme et les autres parties prenantes.

La mise en œuvre de ce principe a les implications suivantes :

- ✓ Mettre en œuvre des mesures de sécurité suffisantes afin d'assurer la continuité du service;
- ✓ Veiller à ce que les données sensibles soient protégées de façon adéquate;
- ✓ Évaluer la sécurité de toutes les organisations concernées dans la chaîne de valeur de l'entreprise (ce qui comprend la chaîne d'acquisition des services);
- ✓ Prendre en considération les intérêts des employés dans la conception de la sécurité.

Principe 6 : La sécurité de l'information nécessite des efforts pour sa compréhension et pour favoriser l'engagement

La connaissance des menaces pour la sécurité est essentielle à la capacité d'une organisation à gérer les risques. Un niveau élevé de sensibilisation dans ce domaine dans l'organisation favorise une « culture de la sécurité » et peut réduire la fréquence et les effets des incidents de sécurité de l'information. Une sensibilisation étendue dans l'organisation est nécessaire pour l'ensemble du personnel, et la connaissance et la compréhension approfondies des menaces sont nécessaires pour le personnel ayant des responsabilités en sécurité de l'information. La connaissance de la sécurité de l'information vient directement en aide aux organisations en permettant :

- ✓ D'instaurer une « culture de la sécurité » au sein du personnel de l'organisation;
- ✓ De favoriser la détection précoce des menaces pour la sécurité de l'information;
- ✓ De faciliter l'acceptation des politiques de sécurité de l'information;
- ✓ D'améliorer la communication au sein de l'organisation au sujet de la sécurité;
- ✓ De coordonner plus efficacement les réponses aux incidents de sécurité;
- ✓ D'obtenir une excellente connaissance des vulnérabilités et des menaces de sécurité; et
- ✓ D'obtenir un niveau élevé de soutien en matière de sécurité de l'information de la part des différentes entités de l'organisation.

La mise en œuvre de ce principe a les implications suivantes :

- ✓ Concevoir et maintenir à jour la politique et le cadre de gestion de sécurité de l'information de l'organisme;

- ✓ Mettre en place des programmes de sensibilisation et de formation adaptés à l'organisation et aux rôles des employés de l'organisme et de ses fournisseurs, lorsque requis dans ce dernier cas;
- ✓ Intégrer la sécurité de l'information dans les processus de communication existants;
- ✓ Participer à des réseaux informels et formels de partage l'information.

Principe 7 : La sécurité de l'information est basée sur un processus d'amélioration continue

Comme l'exposition de l'organisation au risque est constante et changeante, la revue et l'amélioration de la sécurité de l'information doivent faire partie des pratiques courantes des organismes. Une bonne gouvernance de la sécurité leur permettra de gérer l'écart créé par l'adoption de technologies surpassant les mesures de sécurité mises en place. L'amélioration continue permet à l'organisme de maintenir l'état de sécurité de l'information à un niveau qui soit acceptable pour les parties prenantes, tant internes qu'externes, et maintient le risque de l'organisation à un niveau acceptable. L'amélioration continue permet à l'organisation :

- ✓ De maintenir la capacité d'évaluer les risques de sécurité et de mettre en œuvre les mesures de sécurité requises;
- ✓ De fournir l'assurance que les risques de sécurité de l'information sont identifiés et gérés de la bonne façon;
- ✓ De satisfaire aux exigences légales et réglementaires de manière cohérente;
- ✓ Assurer que les considérations de sécurité sont incluses dans la sélection et dans l'adoption de nouvelles technologies;
- ✓ D'assurer que la performance de l'organisation est maintenue au fil du temps (vérification et évaluation.)

La mise en œuvre de ce principe a les implications suivantes :

- ✓ Assurer que l'expertise et l'expérience en sécurité de l'information sont disponibles pour répondre aux besoins de l'organisation;
- ✓ Apprécier les mesures de sécurité en place en fonction de cadre normatif en sécurité de l'information reconnu internationalement;
- ✓ Mettre en œuvre des systèmes et des processus pour détecter les violations malveillantes ou involontaires de la sécurité de l'information et y répondre;
- ✓ Adapter le processus d'évaluation des risques et de sélection des mesures de sécurité afin qu'il soit alimenté par le processus de gestion des incidents de sécurité;
- ✓ Prendre en compte la sécurité lors de l'évaluation des nouvelles technologies et applications pour l'organisme.

6. Cadre de référence en architecture de sécurité de l'information

Ces travaux ont d'abord porté sur la révision du cadre de référence architectural de l'AGSIN afin de répondre à certaines critiques relatives à son niveau, considéré comme étant trop technique. Une attention particulière a été portée afin d'assurer qu'elle est adaptée aux tendances actuelles de l'industrie et qu'elle répond au nouveau cadre de gestion en RI et en sécurité de l'information, et qu'elle est apte à répondre aux besoins d'intégration à l'architecture d'entreprise.

Pour l'ASIG une démarche de sécurisation systémique (*top-bottom*) a été adoptée. Cette démarche permet la définition de solutions en sécurité de l'information fondées sur la gestion des risques prenant en compte l'ensemble des dimensions de protection (gouvernance, personnes, processus et technologie) et assure la réduction des risques tout en favorisant l'efficacité opérationnelle et le contrôle des coûts de protection.

L'adoption d'une démarche de sécurisation multidimensionnelle pour l'ASIG devrait :

- ✓ Assurer l'alignement des stratégies en RI, du développement et de l'acquisition des actifs ainsi que de la gestion des personnes au contexte de gouvernance et de gestion des risques pour la sécurité de l'information;
- ✓ Mettre en œuvre des solutions globales de sécurité basées sur des mesures de sécurité de gouvernance, des personnes, des processus et des technologies;
- ✓ Élaborer et mettre en œuvre des plans de redondance et de contingence dans le cadre du programme de continuité des activités;
- ✓ Assurer que les mesures de sécurité secondaires sont en place pour répondre à leur défaillance, en évaluant l'impact et le risque de défaillance des points de contrôle de sécurité.

6.1 Démarche de sécurisation

Au cours des dernières années, compte tenu des tendances émergentes telles que la mobilité accrue, l'accès à distance et le nombre croissant de tiers qui ont un accès aux données et aux systèmes des organisations, il est devenu évident que la défense du périmètre de type « Muraille de Chine » comme une panacée à toutes les menaces est incomplète. Par conséquent, il est essentiel pour les détenteurs de l'information et pour les exploitants d'infrastructures critiques d'être en mesure d'élaborer des stratégies de sécurité appropriées reposant entre autres sur la cartographie et sur la compréhension des informations qui doivent être protégées tout au long de leur cycle de vie.

Aujourd'hui, la sécurisation d'un environnement doit reposer sur un ensemble équilibré de mesures de sécurité pour réduire le risque que des éléments internes compromis soient utilisés pour compromettre facilement d'autres éléments, tout en assurant un juste équilibre entre la convivialité et la sécurité. La démarche doit répondre aux besoins en matière de sécurité d'une vaste gamme d'activités opérationnelles, du travail de bureau quotidien en passant par les applications de prestation de services aux citoyens jusqu'au soutien de l'infrastructure de services communs. Pour protéger ces différentes activités, il faut adopter des démarches de sécurité qui font au moins appel aux principales pratiques recommandées.

La défense en profondeur est une démarche systémique (globale) de gestion de la sécurité de l'information basée sur la gestion globale des risques. L'approche de défense en profondeur vise une utilisation collaborative des mesures de sécurité techniques, opérationnelles (qui incluent la sécurité du personnel et la sécurité physique) et de gestion pour atténuer les risques (par ex. : contrôles d'accès techniques pour protéger les bases de données critiques et sécurité physique supplémentaire pour empêcher le personnel non autorisé d'accéder physiquement aux serveurs de base de données).

Le concept repose, à l'origine, sur une stratégie de la doctrine militaire qui prône la mise en œuvre de moyens de défense à un niveau suffisant pour retarder plutôt que pour empêcher la progression d'un attaquant. Elle est basée sur l'axiome selon lequel, au fil du temps, une attaque perd de son efficacité, ce qui permet à ceux qui font l'objet de l'attaque de répondre de façon appropriée. La défense en profondeur est beaucoup plus qu'un concept informatique, car elle propose une approche qui permet de :

- ✓ Prendre des décisions fondées sur la gestion des risques;
- ✓ Favoriser l'amélioration de l'efficacité opérationnelle;
- ✓ Réduire à la fois les risques et les coûts de protection et de défense, tout en améliorant la sécurité de l'information.

Une défense basée sur une stratégie de protection en profondeur exige d'abord la compréhension de l'environnement, de la criticité du système, des processus et des informations pour les activités d'une organisation. Dans cette approche, la détermination de la valeur des actifs informationnels est essentielle pour obtenir les avantages de cette approche.

La mise en œuvre d'une stratégie basée sur la défense en profondeur comprend :

- ✓ Une analyse des préalables, qui cible les intrants à mettre en place pour la mise au point d'une défense robuste dans le cadre de l'application d'une stratégie de défense en profondeur;
- ✓ Une analyse des risques, qui met en application une approche méthodologique d'analyse afin de déterminer les éléments essentiels devant être pris en compte pour l'évaluation de l'état actuel de la sécurité;
- ✓ La sélection des mesures de sécurité, qui utilise un référentiel de mesures de sécurité de gouvernance, des personnes, des processus et des technologies.
- ✓ La détermination des conditions d'assurance, qui aborde les considérations et les moyens à mettre en place afin d'assurer le maintien de la pertinence de la stratégie de défense en profondeur.

La défense en profondeur doit être complémentée par les approches suivantes :

- ✓ La sécurité par couches, car elle permet de s'assurer que les différentes couches technologiques d'un système d'information (applications, bases de données, plateformes, intergiciels et communications) sont protégées de manière adéquate. Elle réduit le risque qu'une faiblesse d'une partie du système soit exploitée de façon à ce que les mesures de protection des autres parties soient contournées;
- ✓ L'attribution des privilèges d'accès minimal : attribution aux utilisateurs du droit d'accès minimal nécessaire à l'exécution de leurs tâches (p. ex. : exécution des tâches quotidiennes avec des comptes d'utilisateur à usage restreint, et non avec des comptes administratifs);
- ✓ Le suivi basé sur la prévention, la détection, l'analyse, la réaction et la reprise permet de veiller à la détection et au confinement des attaques réussies, à la restauration des actifs informationnels à un état sûr et authentique ainsi qu'à la documentation et à l'utilisation des leçons apprises pour améliorer la posture de sécurité de l'organisation.

L'adoption de cette démarche est reconnue comme concourant à une saine gestion de la sécurité de l'information dans une organisation en proposant une approche raisonnée pour documenter une stratégie de sécurité adaptée au contexte des organisations et apte à apporter une réponse suffisante aux risques tout en assurant l'efficacité opérationnelle et la prise en compte des coûts.

6.2 Modèle de référence en architecture de sécurité

L'intégration de la démarche de sécurisation de la défense en profondeur a nécessité que soit révisé le cadre de référence de l'AGSIN et que soit adapté le modèle de référence en architecture de l'AGSIN. Pour y parvenir, un modèle générique a été mis au point, basé sur des caractéristiques communes à un ensemble de référentiels connus en sécurité (l'ISF, Gartner, TOGAF, OSA et Cobit 5). Ce modèle doit favoriser :

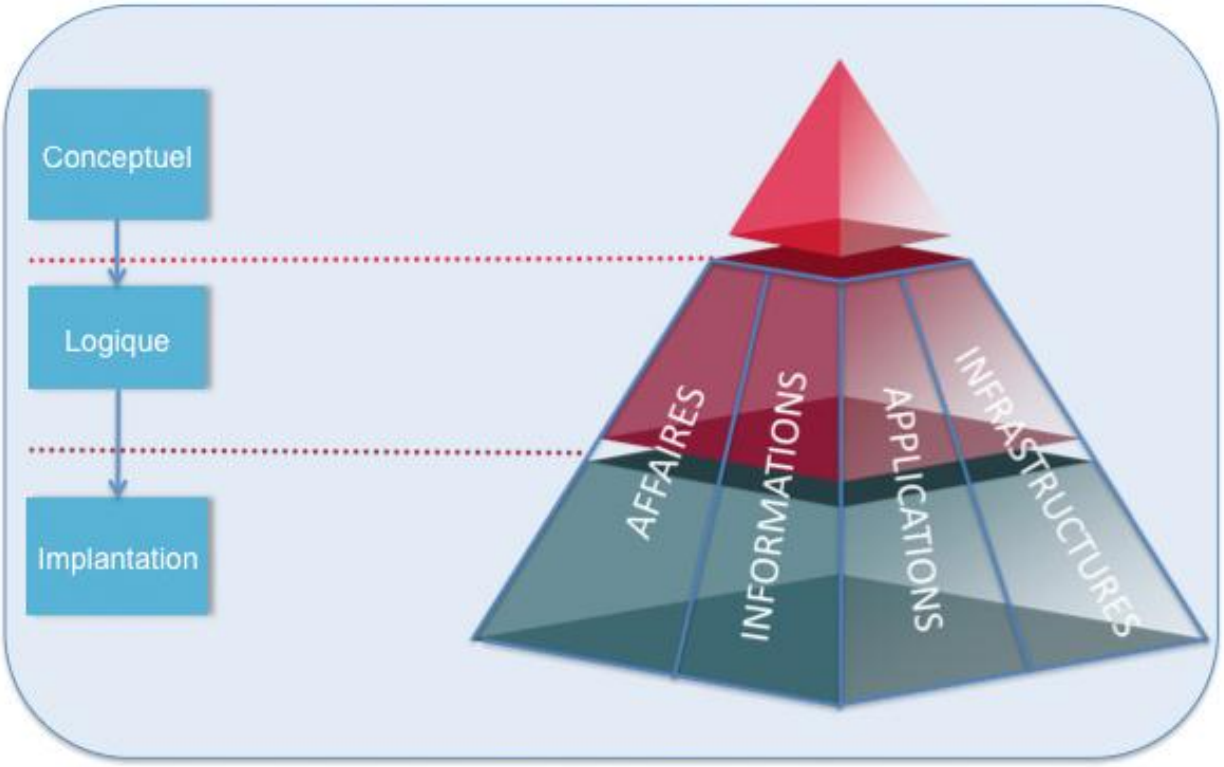
- ✓ L'utilisation de références reconnues afin que soient adaptés les cadres d'architecture des OP;
- ✓ L'interopérabilité entre les OP pour la sécurité tant sur le plan des affaires que sur le plan sémantique ou technique.

Le modèle de référence en architecture proposé s'articule selon trois niveaux d'abstraction et quatre volets. Il s'inspire des travaux de Gartner au sujet de la structure et du contenu d'une architecture de sécurité d'entreprise. Le partitionnement en niveaux d'abstraction représente la notion de planification incrémentale de la sécurité de l'information, chaque niveau présentant plus de détails que le précédent :

- ✓ Au niveau conceptuel, sont établis les orientations, les exigences, les objectifs et les modèles abstraits et peu changeants qui constituent le contexte d'affaires et le cadre normatif de l'organisation;
- ✓ Au niveau logique, sont imaginées les stratégies, méthodes et techniques qui permettent d'atteindre les objectifs de sécurité en tenant compte de l'environnement et des ressources de l'organisation;
- ✓ Au niveau implantation, sont décrits les ressources et les moyens retenus par l'organisation afin que la conception des niveaux précédents soit concrétisée, par acquisition ou par développement.

Selon le degré de maturité de l'ASI d'un organisme et les budgets qui lui ont été consacrés, celle-ci pourra être d'une précision variable à chaque niveau.

Figure 3 : Modèle de référence de l'ASIG (inspiré de Gartner)



La figure 3 présente le modèle de référence en architecture de sécurité. Des informations supplémentaires à son sujet sont disponibles[5].

Au niveau conceptuel, le modèle propose la prise en considération de l'environnement de l'organisation. Ce niveau permet de définir la vision de l'organisation, d'énoncer les principes stratégiques et de définir les exigences et les objectifs en matière de sécurité de l'information. Il vise également à déterminer l'approche de sécurisation et à modéliser l'environnement à sécuriser, à établir les cibles des services de sécurité, à mettre au point des modèles de gestion et déterminer des processus soutenant la sécurité de l'information.

5. Secrétariat du Conseil du trésor, Architecture gouvernementale de la sécurité numérique (AGSIN) (version 1.0), septembre 2001

En d'autres termes, il favorise, à haut niveau, pour un OP, l'articulation d'un programme de sécurité qui couvrira l'ensemble des éléments devant être considéré au niveau subséquent d'architecture de sécurité de l'information de l'organisation.

Au niveau logique, l'architecture de sécurité de l'information gouvernementale suggère aux organismes publics de se baser sur les modèles fonctionnels et les grandes fonctionnalités des éléments de sécurité établies au niveau conceptuel. Ici, on retrouvera notamment des modèles de zones et de niveaux de confiance, d'ententes sur les niveaux de service (SLA), d'échanges d'informations ou encore des modèles relatifs aux applications ou aux infrastructures technologiques. Ce niveau d'abstraction permet également aux organismes d'assurer la cohérence entre le niveau conceptuel et le niveau implantation de l'architecture de sécurité de l'information de l'organisation.

Au niveau implantation, l'architecture de sécurité de l'information gouvernementale regroupe l'ensemble des éléments qui représentent concrètement les moyens retenus par l'organisation afin que soit assurée la sécurité de l'information. On retrouvera, entre autres, les ententes sur les niveaux de service, les divers registres en matière de sécurité (autorité, classification), les divers documents encadrant la gestion opérationnelle (guides et procédures) et la documentation technique (paramètres de configuration logicielle et matérielle).

Le partitionnement en volets, pour sa part, est retenu en raison de la vaste étendue de la sécurité de l'information. Ce partitionnement était aussi conseillé dans l'architecture gouvernementale de sécurité de l'information numérique publiée en 2001[6]. Les volets préconisés représentent différents points de vue sur le modèle de référence.

7. Un environnement à sécuriser

7.1 Enjeux de sécurité

Les nouvelles façons de faire et les fonctionnalités introduites par l'AEG ainsi que les nouvelles tendances en TI donnent lieu à des changements importants à l'environnement gouvernemental actuel. Ces changements s'inscrivent dans la mouvance actuelle en RI, notamment par :

- ✓ La simplification des applications grâce au recours à des interfaces Web de plus en plus utilisées;
- ✓ L'interconnexion croissante à travers des réseaux partagés;
- ✓ La diffusion élargie de l'information gouvernementale;
- ✓ L'utilisation des fonctionnalités du Web 2.0;
- ✓ L'intégration des réseaux voix et données sur des infrastructures simplifiées;
- ✓ L'introduction de l'utilisation de l'infonuagique;
- ✓ L'élaboration et déploiement d'architectures orientées service (AOS);
- ✓ L'utilisation des ressources partagées : infrastructures, applications, capacité de stockage, bande passante, etc. grâce à la virtualisation et à l'infonuagique sous toutes leurs déclinaisons;
- ✓ L'utilisation ou le déploiement de périphériques multifonctions portatifs sans fil (mobilité);
- ✓ Le déploiement d'appareils portables et de réseaux multifonctionnels;

6. Secrétariat du Conseil du trésor, Architecture gouvernementale de la sécurité numérique (AGSIN) (version 1.0), septembre 2001.

- ✓ L'intégration des fonctionnalités de sécurité dans un large éventail de dispositifs informatiques grâce à la croissance des capacités de l'informatique mobile.

Ces modifications architecturales apporteront de nombreux avantages, y compris l'amélioration du service aux citoyens et aux entreprises, l'efficacité opérationnelle et un retour sur investissement plus rapide. Toutefois, ces changements introduisent de nouveaux enjeux de sécurité qui doivent être considérés tant à l'échelle gouvernementale qu'à l'échelle de chaque organisme public dans la constitution ou dans la révision de leurs stratégies et de leur approche de sécurité.

7.1.1 Soutenir les grandes orientations de l'État en RI

Pour soutenir les grandes orientations de l'État, l'architecture d'entreprise gouvernementale (AEG) a établi des cibles d'affaires. Cette section met en évidence celles qui ont un rapport direct avec la sécurité de l'information. Ce rappel des orientations et des exigences architecturales de l'AEG est enrichi de nouvelles orientations ou d'exigences architecturales spécifiques en matière de sécurité de l'information.

Les cibles architecturales énoncées ci-dessous sont tirées de l'AEG. Les exigences ont été regroupées selon trois grands axes, soit :

- ✓ La qualité des services;
- ✓ La performance de l'administration publique;
- ✓ L'innovation dans les RI.

Tableau 1 : Exigences en matière de sécurité associées à la qualité de la prestation aux usagers

Qualité de la prestation aux usagers		
	Exigences d'affaires	**Exigences 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 soutenue par des mesures et des mécanismes qui permettent d'assurer la sécurité de l'information en tout temps et sur l'ensemble du territoire.
Simplicité et convivialité	✓ 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 mesures et les mécanismes de sécurité doivent être simples d'utilisation pour que soit favorisée 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 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 mesures et 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 et des 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'usager.

Tableau 2 : Exigences en matière de sécurité associées à la performance de l'administration publique

Performance de l'administration publique		
	Exigences d'affaires	**Exigences de sécurité**
Efficacité des employés	✓ Accroissement de l'efficacité dans un contexte de réorganisation du travail	Les mesures et les mécanismes de sécurité doivent permettre d'assurer la protection des renseignements personnels durant tout le cycle de vie de l'information.
Caractère concurrrentiel du gouvernement	✓ Réduction des coûts totaux de fonctionnement ✓ Amélioration de l'expertise dans les nouvelles technologies ✓ Projection d'une image d'efficacité et de compétence	La prestation électronique de services permet notamment de rendre disponibles des mesures et des mécanismes reconnus et harmonisés en matière de sécurité de l'information.
Réduction des frais d'exploitation	✓ Coûts totaux de fonctionnement ✓ Économie d'échelle ✓ Coûts de prestation des services ✓ Coûts de gestion des programmes	Les mesures et les mécanismes de sécurité doivent présenter un rapport risques/coûts acceptable.
Contribution du secteur privé	✓ Acquisitions de services infonuagiques ✓ Recours à des partenariats avec l'entreprise privée	L'arrimage entre l'administration publique et l'entreprise privée doit garantir des environnements sécurisés afin de préserver la valeur des actifs informationnels et de protéger les renseignements personnels et la vie privée.
Partage entre les organisations	✓ Intégration de services multiorganisations ✓ Recherche des économies d'échelle ✓ Services partagés et communs	Les solutions envisagées pour simplifier et intégrer les services doivent assurer la sécurité de l'information (cloisonnement, communications sécurisées, etc.)

Tableau 3 : Exigences en matière de sécurité associées à l'innovation en ressources informationnelles

Innovation en ressources informationnelles		
	Exigences d'affaires	**Exigences de sécurité**
Adoption des nouvelles technologies par les individus	✓ Utilisation accrue des NTIC ✓ Échanges et transactions avec le gouvernement ✓ Mobilité ✓ Médias sociaux	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 à inspirer confiance à l'utilisateur. Les mesures et 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 ce que le cadre légal et réglementaire en vigueur au Québec soit respecté et à ce qu'il inspire confiance à l'utilisateur. Les mesures et les mécanismes de sécurité doivent être simples d'utilisation afin de favoriser l'adhésion à la prestation électronique de services.
Adoption des nouvelles tendances en technologie par les OP	✓ Adhésion aux services communs ✓ Le recours à l'infonuagique	Adaptation du cadre de gestion gouvernementale en sécurité de l'information afin d'être en mesure de favoriser l'adoption de ces nouvelles façons de faire en RI.

7.1.2 Sécuriser des environnements technologiques en mutation

L'évolution de l'environnement des affaires et le développement rapide des technologies de l'information et des communications présentent une série de défis pour les organismes publics qui s'appuient sur ces technologies pour assurer leurs opérations au jour le jour. Cette mutation dans les façons de faire, principalement favorisée par une convergence technologique, offre aux OP de nombreux avantages, y compris l'efficacité opérationnelle, la vitesse de déploiement et l'amélioration des services aux clientèles ainsi qu'un retour sur investissement plus rapide.

Toutefois, de nouveaux enjeux de sécurité sont associés à l'élaboration et au déploiement de services Web selon l'approche AOS et à l'introduction des grandes tendances actuelles, et doivent être considérés tant à l'échelle gouvernementale qu'à l'échelle de chaque organisme public dans la constitution ou dans la révision de leur stratégie et de leur approche de sécurité (c'est-à-dire qu'ils doivent prendre en compte les personnes, le contexte organisationnel, les équipements, les infrastructures, l'authentification, l'autorisation, etc.).

Dans ce contexte, l'appréciation des risques reste essentielle, et ce, afin que soient définies les exigences minimales de sécurité à satisfaire et les mesures de sécurité à définir selon les risques anticipés. À titre d'exemple, diverses préoccupations doivent être considérées :

- ✓ Définition de la sensibilité de l'information;

- ✓ Nécessité de reconnaître, de discriminer ou d'identifier et de rendre imputables les utilisateurs accédant à cette information;
- ✓ Nécessité de rendre irrévocable un acte ou un geste accompli;
- ✓ Besoins en matière de persistance et de traçabilité dans le temps;
- ✓ Définition des modalités de réalisation d'audits;
- ✓ Nature de la reddition de comptes en ce qui a trait à la sécurité de l'information;
- ✓ Etc.

Les rubriques suivantes traitent des risques et des principales exigences associés aux vecteurs de la transformation des organisations que sont :

- ✓ L'approche orientée service;
- ✓ L'infonuagique;
- ✓ La mobilité et le prenez vos appareils personnels[7] (PAP);
- ✓ La collaboration sociale;
- ✓ Les mégadonnées[8].

Approche orientée service

On assiste aujourd'hui à l'émergence d'applications basées sur l'architecture orientée service (AOS) afin d'assurer l'agilité et la flexibilité dans la prestation de services. Les cadres de développement basés sur les services Web permettent la réutilisation des fonctionnalités et la création d'architectures distribuées.

À cet égard, le gouvernement du Québec est à élaborer une démarche gouvernementale en ce qui a trait à l'approche orientée service. Elle consiste à définir et à mettre à la disposition des organismes publics un cadre de référence, à fournir un guide d'adoption de l'approche orientée service et à rendre accessibles les mécanismes et les outils nécessaires à la compréhension de ce qu'est une approche orientée service.

Le concept de service est au cœur de cette démarche. Diverses perspectives de l'approche orientée service existent :

- ✓ pour le dirigeant, il s'agit d'un ensemble de services que l'entreprise souhaite exposer à ses clients et partenaires, ou à d'autres acteurs de l'organisation;
- ✓ pour le conseiller en architecture, il s'agit d'un style architectural basé sur la relation entre un prestataire, un consommateur et une description de service, qui présente les propriétés telles que la modularité, l'encapsulation, le découplage, la réutilisation, les services composables et l'orchestration.
- ✓ Il faut donc formaliser le lien entre le consommateur et le partenaire afin que la réutilisation du service en soit facilitée et, s'il y a lieu, que son interopérabilité soit favorisée. On parle alors d'un « contrat de service » dans un contexte AOS : dans le cas où plusieurs partenaires sont concernés, des ententes seront alors nécessaires.

En décloisonnant les applications, l'architecture AOS apporte modularité et évolutivité tout en facilitant l'intégration des systèmes existants aux nouveaux développements. Toutefois, comme l'ont signalé plusieurs auteurs, cette architecture ouverte et répartie a pour conséquence de mettre fin au traditionnel « îlot de sécurité » des applications cloisonnées.

7. En anglais, *Bring your own device* (BYOD).
8. En anglais, *Big Data.*

Les organismes ne peuvent plus gérer la sécurité à l'échelle exclusivement applicative, mais doivent plutôt se concentrer sur des solutions interorganisationnelles qui s'articuleront en fonction des domaines de confiance établis. De la gestion de la sécurité « application par application », on glisse vers une gestion de la sécurité par « domaines de confiance ». La sécurité doit donc être repensée en fonction de cette nouvelle perspective.

Une solution AOS peut être distribuée sur plusieurs domaines de sécurité. Un service peut se composer de différents sous-services se trouvant sous la juridiction de différentes organisations. De plus, les infrastructures de sécurité peuvent varier d'un domaine à l'autre et obliger les utilisateurs à être identifiés à chaque domaine et, conséquemment, plusieurs identités peuvent être rattachées à un utilisateur. Le faible couplage des services associés à une architecture de type AOS met de façon explicite à l'avant-plan la confiance et, en particulier, l'instauration de mesures et de mécanismes assurant la confiance en particulier.

Dans ce contexte, on peut anticiper plusieurs questionnements relatifs à la sécurité, dont, par exemple :

- ✓ Comment vérifier l'identité du prestataire, du partenaire ou du consommateur du service?
- ✓ Comment définir et exposer les droits d'accès à un service?
- ✓ Comment assurer la confidentialité des échanges?
- ✓ Comment assurer la conservation des messages lors d'un échange sensible mettant en jeu plusieurs partenaires?

Ainsi, lors de l'élaboration de l'architecture de sécurité de l'information, des principes propres à l'AOS devront être énoncés. Ces principes, pris en compte dans le domaine de confiance et dans la formulation des ententes de l'organisation, fournissent les fondements pour l'utilisation des standards et de pratiques recommandés, permettant ainsi la formulation des orientations et des lignes directrices concernant l'implantation et l'utilisation des services distribués.

Les principaux enjeux de sécurité :

- ✓ Détermination de la gouvernance des services;
- ✓ Précision de la localisation du catalogue éventuel des services communs (c'est-à-dire emplacement commun permettant aux prestataires de publier des services dans le but d'être recherchés et invoqués par les consommateurs de services;
- ✓ Énoncé du contrat de service accompagnant le service lors de son exécution (ex. : description des exigences de sécurité, niveaux de service entre le prestataire et le consommateur du service, etc.);
- ✓ Mise au point d'un cadre des exigences.

De façon générale, les solutions dématérialisées (actifs informationnels pouvant être répartis dans divers périmètres internes ou externes à l'organisation) et les services en ligne connaissent une croissance exponentielle. La sécurité des données externalisées par les organisations et les particuliers est donc cruciale. De plus, il faut constater un rapprochement des usages entre vie privée et vie professionnelle, ce qui oblige à repenser la sécurité de l'information.

Infonuagique

L'infonuagique est un modèle permettant un accès réseau sur demande à un bassin configurable de serveurs, d'espaces de stockage, d'applications ou de services TI :

- ✓ Qui peuvent être rapidement mis en fonction et relâchés au besoin (*on-demand*);
- ✓ Qui exigent un minimum d'efforts de gestion ou d'interactions avec le prestataire de ces ressources ou services (libre-service).

De plus, tel que le préconise le *National Institute of Standards and Technology* (NIST), les types de déploiements possibles par l'infonuagique sont les suivants :

Tableau 4 : Types de services infonuagiques acquis

Types de services	Description
Software as a service (SaaS)	Les applications du prestataire sont utilisées à travers le réseau.
Platform as a service (PaaS)	Les applications des clients sont développées et exploitées dans un nuage par l'utilisation des langages et des outils du prestataire.
Infrastructure as a Service (IaaS)	Location de puissance de traitement, de stockage et de réseautique.

Tableau 5 : Types de déploiements des services infonuagiques

Types de déploiement	Description
Public	Les services sont rendus disponibles au public en général ou à de larges groupes d'entreprises indépendantes.
Hybride	Maillage de modes de déploiement (privé ou public). Chaque nuage conserve ses entités uniques. Les nuages peuvent être fédérés ou liés entre eux par la technologie permettant l'interopérabilité des applications.
Privé	Les services sont rendus disponibles pour une seule organisation (chez un prestataire ou à l'interne).
Communautaire	Les services sont rendus disponibles à un nombre limité d'organisations et les utilisateurs y accèdent à travers un réseau privé/public.

La liste qui suit énonce les principaux enjeux de sécurité à prendre en compte :

- ✓ **La localisation des données :** les services d'infonuagique peuvent offrir des ressources informatiques dans des secteurs géographiques adjacents ou éloignés. Les OP doivent considérer les écarts entre les exigences légales et réglementaires du Québec, où elles sont établies, et celles d'autres états sur les plans de la juridiction, de la divulgation des données, des droits de propriété et du maintien de ces droits (cas où les actifs d'un locateur sont considérés comme ceux du prestataire lors d'une faillite).
- ✓ **La gestion du caractère privé des données :** les OP qui utilisent les services d'infonuagique doivent s'assurer que des mesures adéquates de protection de la confidentialité et des données personnelles sont en place.

- ✓ **La confidentialité :** dans un environnement d'infonuagique, l'infrastructure partagée fait fi des paramètres traditionnels de sécurité (cloisonnement). Par conséquent, il faut investir des efforts accrus dans les moyens d'assurer la confidentialité. Il est donc essentiel de protéger les données de nature critique ou de grande valeur lorsqu'elles sont stockées et lorsqu'elles sont en circulation. En outre, les données conservées dans l'infrastructure partagée risquent de ne pas être adéquatement supprimées lorsque les ressources sont attribuées dynamiquement.
- ✓ **La disponibilité :** les ministères et les organismes du gouvernement du Québec doivent être en mesure d'accéder rapidement à leurs données. Le recours aux services d'infonuagique rend les OP tributaires des prestataires sur le plan de la performance réseau. Les auteurs de cybermenaces peuvent paralyser un prestataire d'infonuagique au moyen d'attaques par déni de service et de propagation de maliciels ou encore craquer une clé de chiffrement en monopolisant la majeure partie de la puissance de traitement dudit prestataire. La disponibilité des serveurs appartenant aux prestataires peut avoir des répercussions sur le rendement et sur le temps d'attente des applications gouvernementales, ce qui peut entraîner des interruptions de service ou des retards de traitement excessifs.
- ✓ **L'intégrité et le contrôle des accès :** sans l'application de mesures robustes d'authentification et de contrôle des accès, les entités internes malveillantes, les employés des prestataires d'infonuagique ainsi que d'autres auteurs de menaces pourraient être en mesure de mettre la main sur des identifiants et des mots de passe du gouvernement du Québec. Forts de ces informations, les auteurs de menaces peuvent accéder à des comptes ou les utiliser à des fins illégales ou malveillantes, entraînant ainsi la perte de maîtrise des services et des données sensibles. La gestion de l'identité (ex. : l'utilisation de services infonuagiques par les entreprises et les organisations) stimule le besoin de recourir à un service de gestion de l'identité et des accès ou à des courtiers d'identité (*identity bridge*) pour faciliter l'approvisionnement des utilisateurs, l'accès unifié aux actifs informationnels, la fédération d'identités et, le cas échéant, la certification de l'identité des utilisateurs);
- ✓ **L'environnement multilocataire complexe et les fuites de données :** généralement, les prestataires de services d'infonuagique utilisent des infrastructures et des services que se partagent plusieurs prestataires, ce qui leur permet de faire des économies considérables tout en permettant que les ressources soient dynamiquement attribuées en fonction des besoins des clients. Les environnements où les ressources sont partagées entre plusieurs prestataires comportent des risques de fuites de données à la suite desquelles des clients peuvent avoir accès aux données d'autres clients. De plus, lorsque les données de clients ne sont pas adéquatement cloisonnées, il y a un risque important de propagation des maliciels entre les clients.
- ✓ **La perte de données :** des données pourraient être perdues à la suite de suppressions accidentelles causées par des prestataires d'infonuagique, des désastres naturels ou des suppressions volontaires causés par des intervenants malveillants ou des auteurs de menaces. Le prestataire devrait jouer de prudence en faisant des copies de sauvegarde des données et en les protégeant contre la compromission ou la corruption. Au reste, les OP devraient demander des exportations périodiques de leurs données, de sorte qu'une copie de celles-ci puisse être conservée dans leur propre réseau.
- ✓ **La gestion de la chaîne d'approvisionnement :** à l'instar des autres technologies, les produits d'infonuagique peuvent être vulnérables à la malversation ou aux altérations. Ainsi, d'éventuels problèmes concernant l'intégrité de la chaîne d'approvisionnement doivent être pris en compte.
- ✓ **Les interfaces de programmation d'applications (API) non sécurisées :** une API est une interface logicielle qui permet à deux applications de communiquer entre elles. De nombreux services subordonnés à l'infonuagique, notamment la prestation, la gestion et la surveillance, sont tributaires des API. Les API qui sont conçues sans que la sécurité soit prise en compte peuvent constituer des brèches exploitables par des auteurs de cybermenaces qui cherchent à atteindre des données critiques.

- ✓ **La gestion du chiffrement des informations en transit :** au repos et des clés cryptographiques.

Collaboration sociale

L'utilisation des réseaux sociaux d'entreprise ainsi que des médias sociaux n'est pas nouvelle, mais elle se généralise. Certaines particularités doivent être considérées dans la collaboration sociale, comme l'ouverture, la transparence, l'honnêteté, la confiance et la réputation, notamment.

Différentes utilisations deviennent possibles par l'entremise de la plateforme collaborative (où, par ailleurs, différentes entités pourraient être parties prenantes dans la collaboration), comme le partage de documents, la conversation, la recherche (veille), la diffusion ou encore la co-création. À cet effet, le réseau social d'entreprise devient l'agrégateur permettant à la fois l'accès aux applications de mission de l'organisation, aux informations structurées et non structurées (voix, données, images, vidéos), mais aussi permettant l'usage du courriel et de la messagerie instantanée.

Également, cette tendance met de la pression sur les organisations pour qu'elles acceptent des identités numériques professionnelles (LinkedIn, Twitter, etc.) ou personnelles (Facebook, Google, etc.) lors de l'inscription ou de l'authentification pour accéder à des prestations électroniques de services d'une entreprise ou d'une organisation.

Les principaux enjeux de sécurité de la collaboration entraînent la complexification des processus d'affaires auxquels il faut ajouter des activités de collaboration. De plus, différentes entités peuvent être parties prenantes sur un actif informationnel. La collaboration implique, entre autres, la confiance, la réputation et l'identité ainsi que l'application des règles de sécurité par les participants, et oblige les organisations à prévoir les règles de collaboration, à déterminer son cycle de vie.

Il est prioritaire d'élaborer une stratégie de sécurité et une gouvernance de la collaboration sociale dans l'organisme tenant compte :

- ✓ Des objectifs d'affaires;
- ✓ De la propriété, de la sécurité et de la fiabilité de l'information publiée;
- ✓ De l'image de marque;
- ✓ De l'éthique, de la vie privée et de la protection des renseignements personnels;
- ✓ Des besoins en matière d'identification et d'authentification;
- ✓ De la nouvelle réalité en ce qui a trait à la cybersécurité.

Mobilité et mode prenez vos appareils personnels (PAP)

Gartner prévoit que d'ici 2017, 25 % des entreprises se seront dotées d'applications mobiles internes (un équivalent à l'*App Store*). L'écosystème de la mobilité au sein du domaine de confiance d'un organisme public reposera sur divers éléments, entre autres :

- ✓ L'utilisateur;
- ✓ L'équipement mobile (matériel, système d'exploitation et applications);
- ✓ Les PES soutenant la mobilité;
- ✓ L'infrastructure de l'organisation (serveurs, services et applications, données);
- ✓ Le réseau (connexion des équipements mobiles à l'organisation, la prise en charge du WiFi ou du cellulaire, etc.).

L'utilisation de dispositifs mobiles (ex. : tablettes, ordinateurs de table, portatifs, etc.), sous le contrôle ou non de l'organisation, ouvre de nouvelles possibilités et de nouveaux défis en sécurité, en particulier en matière d'identification et d'authentification d'utilisateurs mobiles.

Par ailleurs, la mise en œuvre d'une stratégie de PAP, lorsque retenue, devra s'inscrire dans la stratégie d'ensemble de mobilité de l'organisme. L'objectif ici est de favoriser l'emploi de terminaux mobiles personnels pour accéder aux données de l'organisation : des défis existent donc quant au contrôle des équipements, à la sécurisation des contenus, mais aussi des applications accessibles par l'entremise de ces équipements.

Enjeux de sécurité

Les dispositifs mobiles sont dotés de capacités informatiques puissantes et peuvent communiquer avec des réseaux WiFi, des réseaux cellulaires et tout autre dispositif au moyen de protocoles comme Bluetooth. L'utilisation des technologies sans fil facilite l'accessibilité et la collaboration, en raison de la commodité, de la souplesse et de la mobilité qu'elles offrent. Les dispositifs mobiles et les signaux sans fil sont des éléments clés dans l'atteinte de cet objectif, mais ils peuvent constituer une menace pour l'information gouvernementale et les actifs informationnels, puisque les auteurs de menaces ciblent fréquemment les OP et leurs réseaux pour obtenir de l'information sur les employés, sur les projets et sur les systèmes de l'État québécois.

Les dispositifs mobiles sont aussi vulnérables aux mêmes types de cybermenaces que les ordinateurs traditionnels, dont les maliciels, les logiciels espions et les chevaux de Troie. Le fait de permettre l'utilisation de dispositifs à capacité sans fil pour accéder à des renseignements critiques ou classifiés peut entraîner une exfiltration (fuite) de données électroniques ou vocales. L'exfiltration peut être intentionnelle ou non, et être effectuée au moyen d'un implant installé dans le dispositif par l'auteur d'une attaque.

En ce qui à l'utilisation de ces équipements en mode PAP, la menace d'exfiltration est amplifiée lorsqu'un dispositif du gouvernement du Québec peut être connecté par inadvertance ou intentionnellement à un réseau n'appartenant pas à celui-ci ou servir de pont entre un réseau sans fil externe et un réseau du gouvernement, fournissant ainsi une voie de transmission pour l'exfiltration.

Il est important que les OP insistent sur :

- ✓ Le respect du cadre d'utilisation établi par l'organisation et la séparation des données personnelles;
- ✓ L'adaptation (pour l'organisme public) de la politique de sécurité de la mobilité et du PAP et la précision du cadre d'utilisation de ces équipements (ex. : énoncé des règles concernant le type de support autorisé);
- ✓ Le recours aux dispositifs (gérés ou non) à des fins d'identification et d'authentification : les dispositifs peuvent se révéler intrusifs envers son propriétaire, car il fait appel à des données de géolocalisation, de référencement personnel ou professionnel et d'autres données critiques et pouvant porter atteinte à la vie privée.

Mégadonnées

Les données affluent et les objets connectés (reliés à Internet) sont de plus en plus nombreux (Internet des choses). Ces informations arrivent parfois en temps réel, en continu et sont souvent de type non structuré (ex. : données, images, sons, voix). En ce qui a trait aux informations liées à l'identité d'une personne, il s'agit de données critiques dans un contexte de décloisonnement (PES multipartite) et de délocalisation (services déployés dans l'infonuagique) des actifs informationnels.

Cela soulève un certain nombre de préoccupations quant au traitement grandissant du volume de ces données (ex. : Faut-il tout sauvegarder et tout analyser?).

Les enjeux de sécurité associés à cette technologie sont :

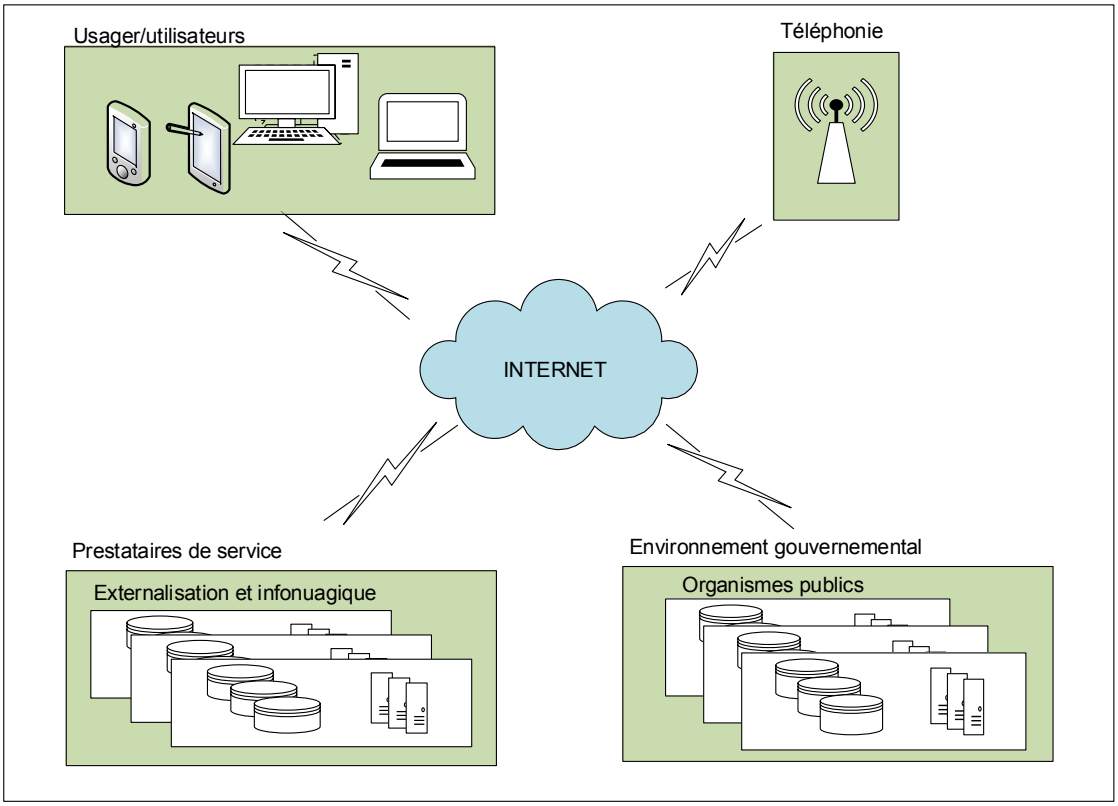
- ✓ Les modalités de gouvernance et de gestion des données (ex. : localisation, stockage, etc.);
- ✓ La gouvernance adéquate pour les données spécifiques à l'identité (ex. : doivent être gérées rigoureusement pour en assurer la qualité, et leur utilisation doit s'effectuer de façon

systématique et formelle, en fonction du niveau de confiance requis envers l'identité et du contexte d'utilisation).

7.1.3 Adapter la sécurité aux nouveaux usages

Toutefois, comme l'illustre la figure 4, l'adoption de ces technologies et de nouvelles approches en RI ainsi que la mise en place de ces nouveaux environnements permettent un large éventail de communications avec l'externe et de possibilités d'échange et de diffusion des informations. Des informations critiques des organismes se retrouvent maintenant sur les ordinateurs portables, des assistants numériques personnels (ANP), des clés USB, des disques durs portables, des appareils mobiles, dans des infrastructures virtualisées, chez des prestataires de l'infonuagique. Ces composants existent souvent en dehors de la définition traditionnelle du périmètre de sécurité des organisations. En plus, ce périmètre s'agrandit pour que soient inclus les citoyens, les entreprises, les prestataires, les partenaires, les mandataires et le personnel mobile.

Figure 4 : Dépérimétrisation et convergence des technologies



Ces changements ont des répercussions importantes sur le périmètre de sécurité traditionnel des organisations. La suppression des barrières de sécurité des organisations auparavant strictement définies et séparées présente des défis importants, comprenant :

- ✓ La dégradation potentielle de la qualité de service découlant du partage d'infrastructures;
- ✓ La complexité des environnements distribués à laquelle s'ajoutent les difficultés de mise en place des mécanismes d'authentification et d'autorisation;
- ✓ L'augmentation de la surface d'attaque des réseaux et des systèmes;

- ✓ La combinaison des vulnérabilités et la création de nouvelles vulnérabilités tributaires de la convergence de technologies auparavant distinctes (par exemple, informatique et téléphonie);
- ✓ L'accroissement de la dépendance aux infrastructures informatiques à un point où de nombreux OP ne peuvent se permettre de pannes prolongées de leur infrastructure informatique sans subir des conséquences graves;
- ✓ La confusion en ce qui concerne l'attribution des responsabilités et la reddition de comptes pour la protection des données, y compris les ambiguïtés de compétences juridiques créées par le développement de l'informatique en nuage;
- ✓ La complexification de la gestion des incidents et des interventions dans des environnements interconnectés avec de nombreuses parties prenantes externes; et
- ✓ Le besoin accru d'assurer une bonne gestion des situations où l'information organisationnelle est détenue par des tiers (par exemple, par la réalisation d'audits de conformité ou l'exigence de soumettre régulièrement des rapports de conformité).

La multiplication des appareils téléphoniques intelligents et des tablettes dans les organisations obligent ces dernières à repenser leur politique de gestion et de sécurité. Le problème est que le service informatique doit faire face à la multiplication des plateformes mobiles qui ne sont pas toutes égales sur le plan de la sécurité. Cette diversification donne à elle seule une idée des changements nécessaires dans les organisations, qui doivent trouver les bons outils pour sécuriser les terminaux mobiles multisystèmes d'exploitation : effacement des données à distance, verrouillage à distance, activation d'un accès par mot de passe, cryptage, authentification, mise en place d'un pare-feu, antivirus et RPV mobile.

Ces environnements sont souvent critiques et particulièrement à risque d'interruption des opérations ou d'attaques aux infrastructures. Cela peut conduire à des perturbations des opérations entraînant des répercussions économiques et sociales importantes. Par conséquent, il est essentiel pour les responsables et les exploitants d'infrastructures gouvernementales critiques d'élaborer des stratégies appropriées pour la cartographie et la compréhension des couches d'informations détenues dans leur environnement et sur les réseaux informatiques qui doivent être protégés.

Avec ces nouveaux environnements, la protection de l'information gouvernementale (à la fois physique et électronique) contre la fuite, la destruction ou la modification accidentelle ou illicite est devenue de plus en plus difficile. Le défi que pose la multiplication des usages, notamment par l'entremise des terminaux personnels (téléphones intelligents et tablettes), des réseaux sociaux et des services infonuagiques, doit alerter les responsables en RI et les responsables de la sécurité ainsi que les dirigeants des OP sur la nécessité d'engager une nouvelle politique de sécurité pour contrer les menaces.

L'arrivée de l'infonuagique et de la « consumérisation » des TI forcent les OP à adapter leur approche liée à la sécurité. Pour cela, il ne suffit pas de déployer uniquement des solutions techniques. Il faut établir une vraie gouvernance sur la gestion des risques. Les responsables ne doivent donc plus seulement avoir une approche tactique ou partielle de la sécurité (technique), mais doivent adopter une approche stratégique. Il faut adapter la sécurité en fonction des usages, des informations vitales et des identités. Cela passe par une gouvernance et par la gestion des risques. Une gouvernance efficace exige une définition claire des objectifs de l'OP ainsi que des éléments représentant le mieux ce programme, à savoir les réglementations, les stratégies, les processus, les normes applicables et les technologies.

Il est nécessaire de mettre au point un cadre de gouvernance efficace pour gérer les risques de sécurité et répartir les responsabilités. C'est le processus de création et du maintien d'un cadre, des structures de soutien et des processus de gestion qui donnent l'assurance que les stratégies de sécurité de l'information sont alignées et qu'elles appuient les objectifs organisationnels. Un cadre de gouvernance de sécurité adapté est essentiel pour le développement d'une « culture de la sécurité » dans l'organisation et pour permettre à l'organisation de gérer efficacement la sécurité pendant les périodes de changement. Le cadre de gouvernance permet de prévoir un certain nombre de stratégies pour atteindre une gouvernance de la sécurité forte compte tenu du contexte actuel caractérisé par l'écart croissant entre la vitesse d'adoption de la technologie et celle de la mise en place d'environnements adéquatement sécurisés (par la mise en œuvre des mesures de sécurité).

Les principaux éléments d'un cadre comprennent :

- ✓ La gestion des risques de sécurité;
- ✓ La mise en place des politiques de sécurité;
- ✓ La définition des rôles et des responsabilités de sécurité;
- ✓ L'adoption d'une démarche de sécurisation globale et structurée en matière de sécurité;
- ✓ L'identification des solutions globales de sécurité (gouvernance, personnes, processus et techniques);
- ✓ La sensibilisation et la formation du personnel.

7.1.4 Favoriser un investissement équilibré en sécurité

Finalement, un enjeu de taille à gagner : l'investissement équilibré en sécurité de l'information. La sécurité totale de l'information ou, dit autrement, le « risque zéro », sur l'information, n'existe pas. Le défi du domaine de la sécurité de l'information consiste essentiellement à maintenir un équilibre délicat entre les mesures de sécurité nécessaires pour atteindre un risque résiduel considéré comme étant acceptable sur les informations d'une organisation et les coûts acceptables que les investissements à cet égard engendrent. La question est : « Comment une organisation peut-elle y arriver? ».

La mise en place d'un programme de sécurité de l'information adapté aide les organisations à assurer la protection des informations et des renseignements personnels qu'elles détiennent tout en veillant aux intérêts des parties prenantes et à maintenir l'équilibre entre le risque, les coûts et la qualité des services. Une structure de gouvernance efficace doit définir les responsabilités, les stratégies, les principes clés de sécurité et les actions d'une organisation pour s'assurer que ses objectifs sont atteints. La définition des architectures de sécurité de haut niveau afin que soit assuré l'ordonnancement des différents éléments de sécurité est utile pour atteindre cet objectif.

Enfin, c'est là que les plans de l'architecture de la SI présentés dans ce document viennent donner des réponses aptes à guider la communauté gouvernementale dans la sécurisation de ses informations.

7.2 Approche de sécurisation

Dans les dernières années, le décloisonnement entre les organismes publics s'est répandu au sein du gouvernement du Québec. En effet, la maturité et la démocratisation des technologies de l'information ont modifié de façon marquée la portée et la nature des prestations électroniques de services. À titre d'exemple, les utilisateurs (citoyens, employés, etc.) requièrent de l'instantanéité (accès rapide aux services, informations en temps réel), les organisations se centrent sur le client et la collaboration sociale émerge tant à l'interne qu'à l'externe de l'organisation.

Les nouvelles tendances limitent l'efficacité du modèle de protection centralisé. Avec la mobilité, l'usager ou l'utilisateur et ses équipements ne sont plus dans le périmètre. Avec l'infonuagique, les actifs informationnels ne sont pas dans le périmètre. De la même manière, pour les applications distribuées, le client et le service ne sont pas dans le même périmètre.

De plus, avec l'émergence des nouvelles tendances en RI, il faut connaître les limites des différentes solutions de sécurité, car les niveaux de confiance peuvent varier selon :

- ✓ La localisation des informations;
- ✓ La nature des PES ou le type des transactions;
- ✓ L'ubiquité des accès avec la collaboration, l'usage des réseaux sociaux et les équipements de la mobilité;
- ✓ Le niveau de sécurité des environnements des prestataires de services;
- ✓ Le rôle de l'utilisateur et des usagers.

Dans ces nouveaux environnements, la sécurité est très dépendante du contexte et de la confiance rattachée au contexte. Le nouveau modèle de sécurité repose toujours sur l'appréciation des risques, mais il doit garantir la sécurité des services distribués, des services acquis des prestataires de l'infonuagique, la protection des terminaux et la supervision de la confiance, principalement par la mise en place de mécanismes d'assurance de la sécurité obtenus par l'examen ou par l'audit de la sécurité et la certification des tiers, lorsque requis.

Le nouveau modèle de sécurité « dépérimétrisé », plus particulièrement pour le modèle de confiance, doit prendre en compte :

- ✓ Les personnes, les organisations, les équipements, les infrastructures;
- ✓ Les différents niveaux de confiance, qui peuvent varier selon la localisation, le type des transactions, le rôle de l'utilisateur et le risque associé aux enjeux juridiques, à la nature du service acquis ou au type de transaction;
- ✓ L'authentification et l'autorisation, qui doivent soutenir le modèle de confiance;
- ✓ Les exigences de sécurité et la robustesse des mesures qui doivent maintenir les niveaux de confiance requis;
- ✓ L'utilisation étendue du chiffrement des informations;
- ✓ L'implantation de la fédération de l'identité, lorsque requise;
- ✓ La protection des services;
- ✓ La protection des points d'accès et des équipements des usagers;
- ✓ La supervision de la confiance (assurance).

Le concept de domaine de confiance vient préciser la portée de la sécurité. Un domaine de confiance se définit comme étant un ensemble d'éléments d'ordres juridique, gouvernance, processus et technologique, un cadre de gestion et un ensemble d'activités pertinentes assujettis à une politique administrée par une seule autorité en matière de sécurité. La définition d'un domaine de confiance établit les principes et les règles de gouvernance et de gestion, les exigences, les mesures concernant les actifs informationnels d'un environnement défini par la portée d'une politique de sécurité.

Le modèle traditionnel d'imputabilité quant à la sécurité de l'information et à la protection des renseignements personnels consiste à confier la responsabilité à l'organisme public détenant l'information. Ce modèle a soulevé dès l'origine plusieurs questions, particulièrement dans le cadre d'un service ou d'un échange engageant plusieurs OP. Par exemple :

- ✓ Quelles sont les responsabilités de chacun des OP participants et quelles sont leurs limites?
- ✓ Y a-t-il une autorité imputable et comment la détermine-t-on? Comment faire appliquer l'autorité retenue?
- ✓ Qui est responsable de la définition des mesures de sécurité lorsque des informations sont partagées par plusieurs OP?
- ✓ Quelles personnes ou organisations, quels systèmes ou équipements ou quelles informations peuvent être des sources de données fiables à des fins précises et comment cette fiabilité est-elle déterminée?
- ✓ Quelles personnes ou organisations ou quels systèmes sont suffisamment dignes de confiance pour recevoir des informations à des fins précises?

Le concept de domaine de sécurité composé d'une autorité basée entre autres sur une politique de sécurité et un cadre de gestion va permettre d'assurer l'harmonisation et l'interopérabilité des façons de faire des OP utilisateurs de services partagés ou des participants à l'échange. Il vient donc préciser la portée de la gouvernance en matière de sécurité.

Enfin, ce concept permet aux OP utilisateurs d'un service partagé ou des participants à un échange, sous la responsabilité d'un domaine de confiance, de bien exprimer les exigences requises en ce qui a trait à la sécurité et de bien évaluer les impacts qui les touchent.

Les principes du domaine de sécurité représentent les meilleures pratiques et les concepts fondamentaux qui fournissent les bases pour l'utilisation des standards et qui permettent la formulation des orientations et des lignes directrices pour l'élaboration de l'architecture de sécurité de l'information. L'application des principes doivent permettre d'atteindre les objectifs suivants :

- ✓ Faciliter un usage approprié et efficace des moyens de sécurité assurant l'identification, l'authentification, l'autorisation, l'administration et la vérifiabilité en réponse à l'accès et à l'utilisation des ressources informationnelles;
- ✓ Assurer la portabilité entre les plateformes et utiliser les standards ouverts à tout niveau;
- ✓ Soutenir la livraison des services en mode multicanal, lorsque possible;
- ✓ Garantir que les exigences de sécurité et les risques ont été évalués et déterminés adéquatement afin de garantir l'adaptabilité et la disponibilité des ressources informationnelles ainsi que l'accès, la captation et le partage d'informations;
- ✓ Permettre l'introduction ou l'intégration de nouvelles technologies tout en maintenant une protection adéquate de l'information;
- ✓ Gérer et permettre plusieurs niveaux de protection, y compris la protection du réseau, des logiciels systèmes, des applications et des données.

L'utilisation du concept de domaine de confiance, au gouvernement du Québec, permet de prévoir un certain nombre de valeurs ajoutées pour le gouvernement et pour les utilisateurs de ces services.

Plus spécifiquement, les valeurs ajoutées sont les suivantes :

- ✓ L'assurance d'une protection adéquate de bout en bout; cette assurance provient du fait qu'il n'y a qu'une seule autorité responsable du service et à la mise en œuvre du cadre d'exigences;
- ✓ L'amélioration de l'interopérabilité pour la sécurité; un arrimage entre les parties est obligatoire. Ces conditions sont définies dans les ententes, y compris les exigences de sécurité, lesquelles favorisent, pour un service donné, l'interopérabilité de tous;
- ✓ Une délimitation claire des responsabilités et des obligations des intervenants en matière de sécurité;
- ✓ Le respect de l'autonomie des participants dans le choix des mesures et des solutions en matière de sécurité.

En ce qui a trait aux domaines de confiance au gouvernement du Québec, il est retenu de reconduire l'utilisation des domaines et des modèles de confiance dans l'architecture de sécurité de l'information, ce qui est particulièrement utile pour représenter, au niveau conceptuel, le nouvel environnement gouvernemental découlant de la cible de l'AEG et pour formaliser la démarche de sécurisation de l'information.

C'est en effet au niveau conceptuel qu'il est proposé de prendre en considération l'environnement de l'organisation. Ce niveau permet de définir la vision de l'organisation, d'énoncer les principes stratégiques, de définir les exigences et les objectifs en matière de sécurité de l'information. Par la suite, le modèle d'affaires subséquent au niveau logique permettra de représenter la façon dont la sécurité de l'information est pratiquée dans l'organisation ainsi que les interrelations avec le reste de l'organisation (processus, rôles et responsabilités, structures administratives, etc.), éléments essentiels à la constitution des domaines et des modèles de confiance.

Les architectures de sécurité de l'information de chaque organisme public devront préciser (si requis et lors du déploiement, le cas échéant, de nouveaux contextes d'utilisation (ex. : PAP) ou de nouveaux types de déploiement (ex. : infonuagique) :

- ✓ D'une part, au niveau logique, les niveaux de confiance, les ententes sur les niveaux de service, les échanges d'informations ou encore les modèles fonctionnels relatifs aux applications ou aux infrastructures technologiques;
- ✓ D'autre part, au niveau implantation, l'ensemble des éléments qui représentent concrètement les moyens retenus par l'organisation afin d'assurer la sécurité de l'information (ex. : ententes sur les niveaux de service, documents encadrant la gestion opérationnelle (guides et procédures), la documentation technique (paramètres de configuration logicielle et matérielle), etc.).

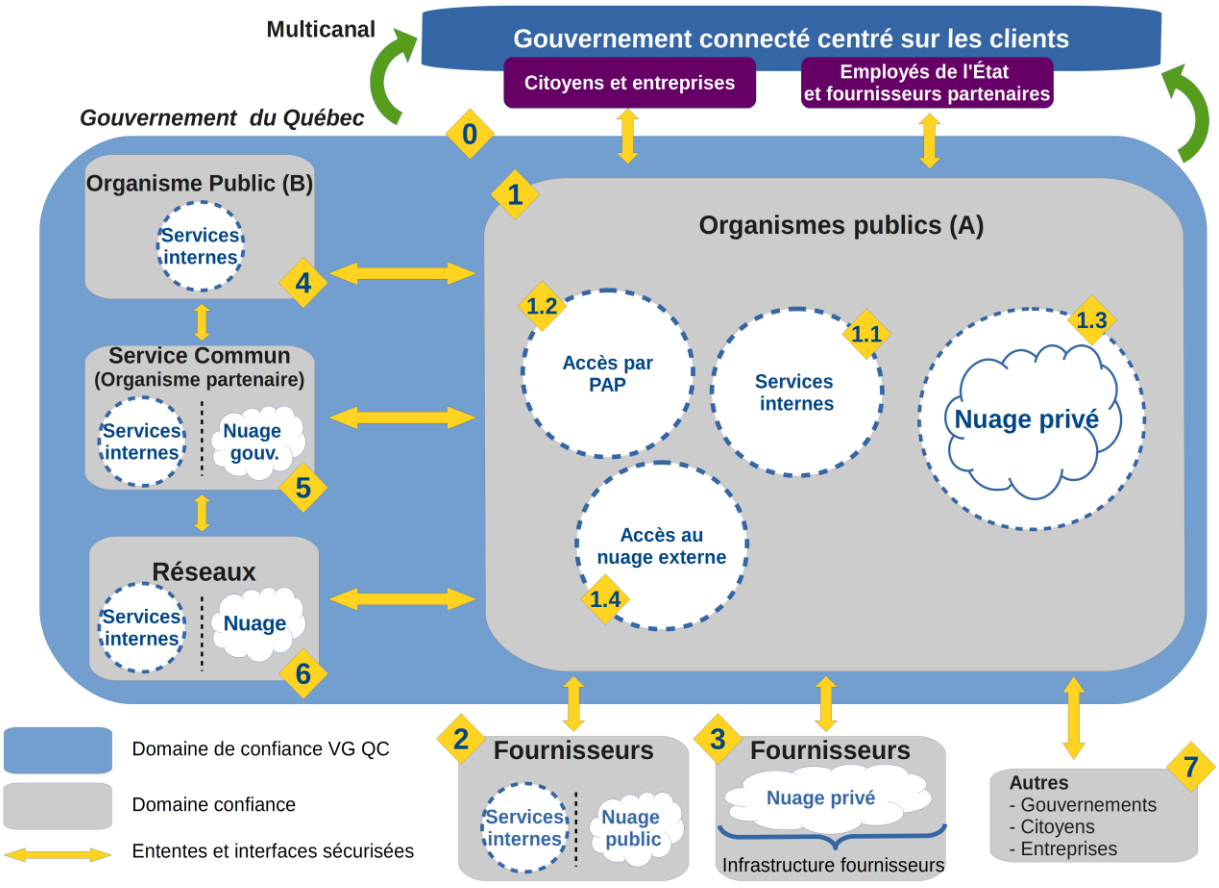
7.3 Modèle global de l'environnement gouvernemental

Cette section illustre à haut niveau les domaines de confiance du gouvernement du Québec en matière de sécurité de l'information.

Les domaines de confiance doivent impérativement prendre en considération l'ensemble des relations (communications, échanges, externalisation) que le gouvernement du Québec décidera d'effectuer au moyen des technologies de l'information. De manière générale, à l'échelle gouvernementale, chaque organisme public établit, dans le cadre de ses activités, les relations 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 (ou avec d'autres paliers gouvernementaux), qui interagit avec l'appareil gouvernemental, mais qui n'est pas sous sa gouverne.

Plus spécifiquement, la figure 5 suivante illustre les domaines de confiance en matière de sécurité pour le gouvernement du Québec.

Figure 5 : Domaines de confiance de l'environnement gouvernemental cible



Le tableau suivant apporte les éléments de précision nécessaires à la compréhension du modèle global des domaines de confiance illustrés précédemment. À chacune des références du modèle est jointe une description sommaire.

Tableau 6 : Description des composantes du modèle global des domaines de confiance

Référence	Description sommaire
Clients	La figure indique les clients (citoyens, entreprises, etc.), soit ceux qui sont concernés par des événements en lien avec les programmes, services et opérations du gouvernement. En guise de rappel, l'énoncé de la vision gouvernementale mentionne : un gouvernement centré sur les citoyens et sur les entreprises, et qui est à la fois efficace et efficient. Plus précisément, la vision de l'État propose un gouvernement centré sur les citoyens et sur les entreprises « qui offre des services accessibles, performants, de grande qualité et sécuritaires à l'ensemble des citoyens et des entreprises du Québec », et qui est à la fois efficace et efficient, « qui répond aux attentes et besoins de la clientèle d'une manière performante en favorisant l'utilisation responsable des ressources collectives gouvernementales ».
0	La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes et des entreprises du gouvernement établit des règles de gouvernance et de gestion en matière de ressources informationnelles applicables aux organismes publics et aux entreprises du gouvernement afin, notamment : ✓ d'instaurer une gouvernance intégrée et concertée, fondée sur la préoccupation d'assurer des services de qualité aux citoyens et aux entreprises de même que de veiller à la pérennité du patrimoine informationnel gouvernemental; ✓ d'optimiser les façons de faire en privilégiant le partage et la mise en commun du savoir-faire, de l'information, des infrastructures et des ressources; ✓ d'assurer une gestion rigoureuse et transparente des sommes consacrées aux ressources informationnelles. Ainsi, le gouvernement du Québec est un domaine de confiance en soi et assume la gouvernance pour l'administration publique.
1	Cette zone représente le domaine de confiance d'un organisme public. On y retrouve tous les services (y compris les services distribués, lorsque requis) ou les échanges liés à sa mission. Chacun (utilisateurs, partenaires et prestataires) est soumis à son autorité, à sa politique de sécurité et à son cadre de gestion de la sécurité.
1.1	Cet élément illustre les services, les ressources, les infrastructures matérielles et logicielles de l'organisme public (A). Ces services peuvent : ✓ engager l'organisme seul; ✓ ou nécessiter un échange avec d'autres organismes publics en vue d'offrir le service. Ce service est inclus dans le domaine de confiance de l'OP, car il fait partie de sa mission et tous les traitements sont effectués par lui. L'OP est responsable de la sécurité de l'information. Les OP participant à l'échange sont liés par une entente et les exigences de sécurité sont clairement indiquées.

1.2	Mode PAP (*prenez vos appareils personnels*) Dans l'hypothèse où un organisme public déciderait de permettre à ses employés d'utiliser des terminaux mobiles personnels pour accéder aux données internes, certains éléments inhérents à la sécurité sont à mettre en évidence. À titre d'exemple, mentionnons : ✓ l'organisme public pourra adapter sa politique de sécurité au mode PAP, préciser le cadre d'utilisation de ces équipements, sensibiliser les employés aux risques encourus, énoncer des règles concernant le type de support autorisé, gérer l'inventaire des équipements ou mettre en place un catalogue (*App Store*) d'applications autorisées; ✓ l'employé serait amené à respecter le cadre d'utilisation énoncé par son organisation, le cas échéant, à signer une entente, à déclarer son équipement, à faire usage seulement des applications approuvées par l'entreprise, à autoriser la prise de contrôle de son appareil, à autoriser un audit de l'appareil ou à gérer adéquatement la séparation de ses données personnelles.
1.3	**Infonuagique privé** (interne) ✓ Les infrastructures et services sont déployés et gérés exclusivement pour l'organisme. ✓ La gestion se fait à l'interne de l'organisme public. ✓ Un bassin de ressources communes peut exister sur le site local. ✓ Il faut prévoir des investissements initiaux pour la mise en place. ✓ L'élasticité est tributaire des investissements. ✓ Des ressources techniques sont à former.
1.4	Dans le cas où l'organisme public fait le choix de recourir à un nuage public ou privé externe, un ensemble d'éléments de gouverne spécifiques devront fort probablement être mis en place. Par exemple, des précisions à la politique de sécurité pour les services infonuagiques (potentiellement des éléments d'ordres technologique et organisationnel supplémentaires), la nécessité d'identifier les utilisateurs internes devant accéder à ces nuages, etc.
2	**Prestataire** ✓ Infrastructures et services à l'OP ✓ Les infrastructures et services sont gérés exclusivement pour l'organisme public (A). ✓ Nuage public ✓ Les infrastructures et les services sont disponibles au grand public (accessibles par des protocoles standards de réseau Internet (navigateur Web)). Les enjeux sont à la fois associés au caractère multilocataire et à la dépendance à la disponibilité du réseau Internet.
3	**Prestataire** ✓ Nuage privé (externe) ✓ Les infrastructures et services sont déployés et gérés exclusivement pour l'organisme public (A). ✓ Gestion par un tiers indépendant (prestataire). ✓ Un bassin de ressources communes peut exister sur le site externe dans un établissement d'hébergement.

4	**Autre organisme public** Cela représente le domaine de confiance d'un autre organisme public (B). On y retrouve tous les services ou les échanges liés à sa mission. Chacun est soumis à son autorité, à sa politique de sécurité et à son cadre de gestion de la sécurité. La présence de ce domaine de confiance a pour objet de représenter les échanges possibles entre un ou plusieurs organismes publics et la nécessité d'établir des ententes entre les domaines de confiance concernés pour les services ciblés.
5	**Services communs** Les services communs peuvent être des infrastructures, des applications ou des sources d'informations. Ces services, assujettis à une autorité qui leur est propre (ex. : ClicSÉQUR), laquelle dicte les conditions d'utilisation de ceux-ci, sont des domaines de confiance en soi. Dans le cas d'un service commun et intégré (ex. : regroupement de services), le niveau de sécurité requis pour ce service intégré est défini notamment en fonction de la catégorisation de l'information et est appliqué à tous les échanges nécessaires au service intégré. Un domaine de confiance spécifique sera déterminé pour ce type de service. Le modèle de référence de l'approche orientée service préconisée par le SCT pourrait engendrer la mise en place de catalogues de services. Il pourrait donc y avoir un catalogue de services communs à la communauté gouvernementale permettant de publier des services recherchés et demandés par les consommateurs de services. Enfin, le mode de déploiement de certains de ces services pourrait être envisagé dans un contexte d'infonuagique, soit dans le cadre d'un nuage gouvernemental.
6	**Réseaux** Les réseaux, regroupements d'OP dans un champ d'activité en particulier, constituent chacun un domaine de confiance. L'autorité sur ce dernier est déléguée à une entité désignée du réseau. Elle est responsable de l'élaboration et de la mise en œuvre des éléments de gouverne qui composent le domaine de confiance.
7	**Entités externes au gouvernement du québec** D'autres entités externes peuvent participer à des échanges avec le gouvernement du Québec. Ces entités peuvent être d'autres paliers de gouvernement de diverses juridictions (ex. : gouvernement fédéral), des municipalités ou des entreprises. Chacune de ces entités a son domaine de confiance.

D'autres types de déploiement dans l'infonuagique, non illustrés ici, seraient également possibles, en conformité avec les normes du National Institute of Standards and Technology (NIST). Les domaines de confiance devraient prendre en considération les exigences de sécurité engendrées par ceux-ci.

Plus précisément, dans le cadre d'un déploiement de type communautaire (c'est-à-dire avec mise en réseau de nuages gérés exclusivement pour une communauté d'organisations ayant des affinités), divers enjeux seront à gérer :

- ✓ Coordination des besoins, des normes et des standards entre les organismes participants;
- ✓ Élaboration du cadre contractuel commun et des niveaux de services;
- ✓ Modèle de gouvernance multiorganisme à mettre en place.

Dans le cadre d'un déploiement de type hybride (c'est-à-dire le maillage de modes de déploiement (privé et public)), anticiper une certaine complexité de gestion, à savoir :

- ✓ Conservation de l'entité unique de chaque nuage;
- ✓ Coordination et échanges entre les différents nuages (fédérés ou liés entre eux par la technologie permettant l'interopérabilité des applications);
- ✓ Établissement d'un modèle approprié de sécurité.

Enfin, la gestion de l'identité, de l'authentification et de l'autorisation (GIA) est à prendre en compte, selon les besoins d'affaires déterminés, par tous les domaines de confiance constitués.

La complexité peut être importante. C'est par exemple le cas dans une situation impliquant des parties prenantes à une prestation électronique de services et des systèmes supportant les actifs informationnels et pouvant appartenir à des domaines de confiance différents. Ces parties prenantes pourraient également appartenir à une autre juridiction, que l'organisme public doit être non seulement en mesure de connaître, reconnaître et autoriser adéquatement et efficacement. Il s'agit également de :

- ✓ S'assurer que ces personnes puissent répondre de leurs faits et gestes, notamment de l'utilisation qu'ils peuvent faire de l'information ou des renseignements qu'ils ont consultés dans le cadre d'une prestation électronique de services donnée;
- ✓ S'assurer que les données fournies et les documents produits par ces personnes ne pourront pas être répudiés par leur auteur, et ce, tout au long du cycle de vie de l'information;
- ✓ S'assurer de la traçabilité des actions faites par ces personnes, peu importe le support utilisé ou le contexte d'utilisation.

8. Vues spécifiques de la sécurité

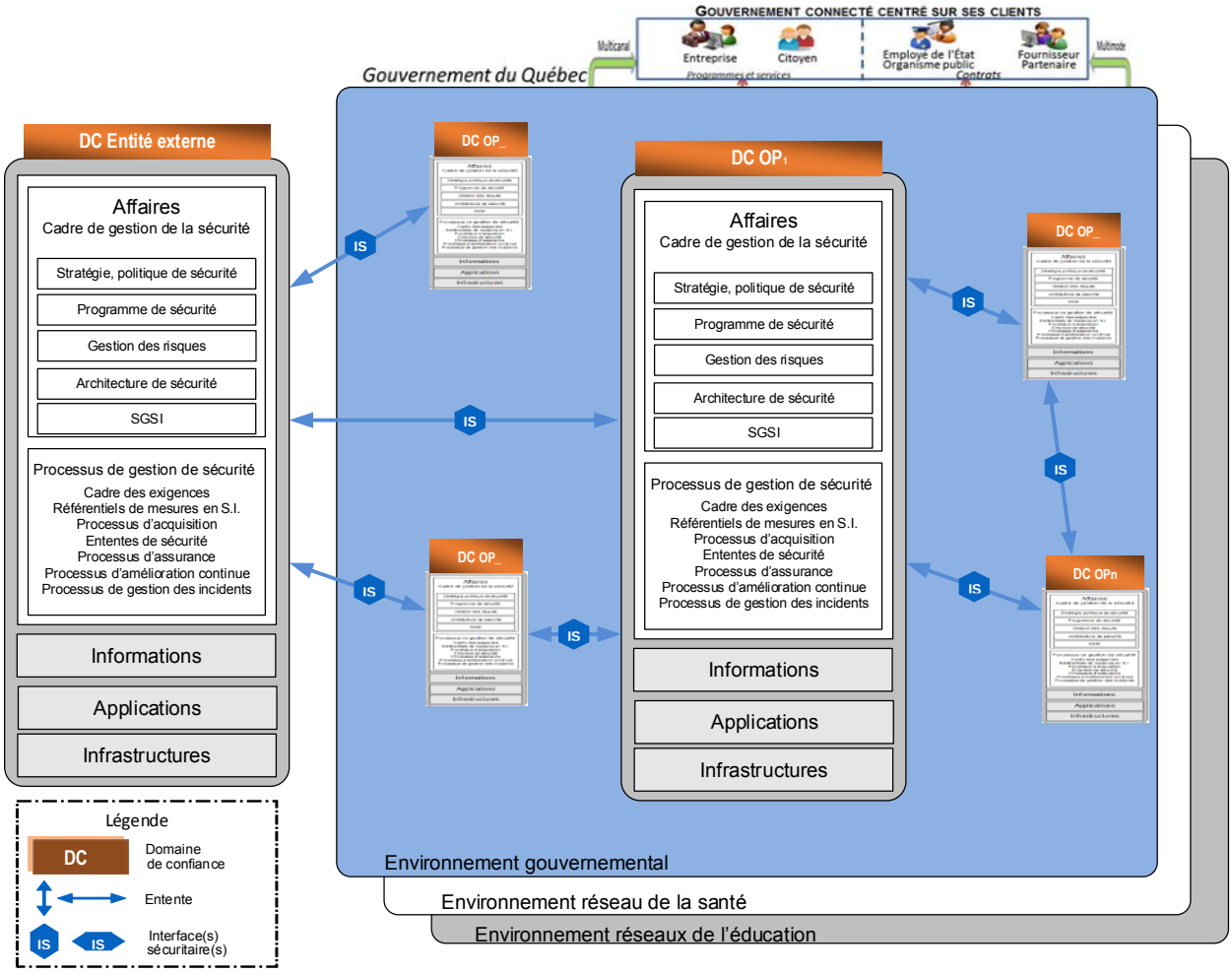
Ces vues permettent de présenter, selon les différents volets de l'AEG, les concepts du modèle général de sécurité et d'évaluer le potentiel de mise en commun, de partage et de réutilisation des ressources en matière de sécurité. Les quatre volets présentés dans cette section sont les suivants :

- ✓ Volet « affaires »;
- ✓ Volet « information »;
- ✓ Volet « application »;
- ✓ Volet « infrastructure technologique ».

Ce découpage en volets respecte le cadre méthodologique en vigueur au sein du Secrétariat du Conseil du trésor et est utilisé pour l'élaboration de l'architecture d'entreprise gouvernementale à haut niveau. En tant que segment de l'AEG, ce document se conforme à cette démarche.

8.1 Volet « affaires »

Figure 6 : Vue « affaires »



Le modèle de sécurité du volet « affaires » présente les composantes de niveau affaires du modèle général présenté à la section 7.3. Pour ce volet, le plan de mise en œuvre devra traiter notamment des processus de gouvernance (gestion des risques, politiques, application, évolution et communication), de gestion de la sécurité et de la reconnaissance des domaines de confiance (guides d'élaboration d'une politique de sécurité, d'un cadre de gestion de la sécurité, d'une entente, d'une interface sécuritaire).

Il permet à une organisation de se doter d'un modèle d'établissement, de mise en œuvre, de fonctionnement, de surveillance, de réexamen, de mise à jour et d'amélioration d'un système de gestion de la sécurité de l'information (SGSI). Ce dernier est destiné à assurer le choix de mesures de sécurité adéquates et proportionnées qui protègent les actifs et donnent confiance aux parties concernées.

La conception et la mise en œuvre du SGSI d'un organisme tiennent compte des besoins, des objectifs, des exigences de sécurité, des processus mis en œuvre, de la taille et de la structure de l'organisme. Ces éléments, ainsi que leurs systèmes connexes, doivent évoluer avec le temps.

On peut cibler plusieurs éléments d'affaires en matière de sécurité qui ont un potentiel de mise en commun, de partage ou de réutilisation. Ces potentiels devront être validés. À titre d'exemple :

- ✓ Mise en commun : ententes et interfaces sécuritaires, cadre d'exigences et référentiel de contrôle et processus d'identification, d'authentification et de signature;

- ✓ Partage : ententes et interfaces sécuritaires des secteurs de la santé et de l'éducation, ententes et interfaces sécuritaires élaborées par les organismes responsables d'une grappe de services, processus propres à un secteur ou à une grappe;
- ✓ Réutilisation : ententes et interfaces sécuritaires des OP, processus propres à un OP.

Lors de l'élaboration de l'architecture de sécurité de l'information, le volet doit traiter des enjeux de sécurité introduits par l'AEG et par les nouvelles tendances. Ainsi, il convient de considérer les enjeux engendrés par ces tendances lors de la constitution des domaines de confiance, de la négociation des ententes, de l'élaboration de la politique de sécurité, de la conception du cadre de gestion, de l'élaboration des ententes avec les partenaires et les prestataires et, aussi, de l'élaboration de l'architecture de sécurité de l'information. Les considérations énumérées aux rubriques suivantes sont en lien avec certains enjeux de sécurité introduits par l'AEG.

Approche orientée service (AOS)

L'approche AOS remet en question l'approche traditionnelle de sécurité, mais il demeure que ces systèmes doivent être protégés contre les menaces tant internes qu'externes. Pour sécuriser une AOS, on doit prendre en compte les enjeux de sécurité suivants : la gestion des identités, la gestion des politiques de sécurité distribuées, l'interopérabilité, la sécurité des messages et la confiance. En ce qui a trait à la gestion de l'identité des services (des dispositifs), il faudra authentifier, autoriser et habiliter les dispositifs à travers différents domaines de confiance. Pour des objectifs de performance, l'implantation de la fédération d'identités sera la solution à privilégier pour les environnements AOS.

Lors de la conception de l'architecture de sécurité de l'information, des efforts devront être consacrés à l'identification de principes guidant l'élaboration des domaines de confiance de l'organisation. Ces principes, du domaine de confiance, représentent les concepts fondamentaux qui fournissent les bases pour l'utilisation des standards et pour l'adoption des meilleures pratiques, et qui permettent la formulation des orientations et des lignes directrices concernant l'implantation et l'utilisation des services distribués. Pour une infrastructure AOS, le domaine de confiance doit :

- ✓ Faciliter un usage approprié et efficace des moyens de sécurité assurant l'identification, l'authentification, l'autorisation, l'administration et l'auditabilité en réponse à l'accès et à l'utilisation des ressources informationnelles distribuées;
- ✓ Assurer la portabilité entre les plateformes et utiliser les standards ouverts à tout niveau;
- ✓ Favoriser la livraison des services multicanal en multimode, lorsque possible;
- ✓ Garantir que les exigences de sécurité et les risques ont été évalués et déterminés adéquatement afin que soient garantis l'adaptabilité et la disponibilité des ressources informationnelles distribuées et leur accès, leur captation et leur partage;
- ✓ Permettre l'introduction ou l'intégration de nouvelles technologies tout en maintenant une protection adéquate de l'information;
- ✓ Gérer et supporter plusieurs niveaux de protection, y compris la protection du réseau, des plateformes, des logiciels systèmes, des applications et des données.

Les principales actions à réaliser sont :

- ✓ Préciser le cadre de gouvernance des catalogues, des services et des sources officielles de données;
- ✓ Déterminer (selon les orientations du SCT) les sources officielles de données du gouvernement du Québec;
- ✓ Identifier les services communs au gouvernement du Québec;
- ✓ Prendre en compte les orientations en matière de gestion de l'identité et des accès (GIA).

Environnement virtualisé

La virtualisation propose de nouveaux types d'environnement de traitement très dynamiques par rapport aux plateformes classiques qui présentent les caractéristiques suivantes :

- ✓ La ressource est une unité physique dénombrable qui interagit avec d'autres unités physiques. À chaque unité physique est associé un ensemble de composantes logiques;
- ✓ La spécialisation des unités physiques à des fonctions précises de traitement : postes clients, serveurs de données, serveurs d'application, imprimantes;
- ✓ le système d'exploitation est la seule composante logicielle qui interagit directement avec le matériel.

Les nouveaux environnements virtuels présentent les caractéristiques suivantes :

- ✓ La virtualisation des ressources est obtenue par la séparation du système d'exploitation des ressources physiques et la séparation de l'application du serveur physique;
- ✓ Une couche de virtualisation, l'hyperviseur, est ajoutée aux unités physiques;
- ✓ La possibilité de créer différents composants virtuels : machine virtuelle, dispositif virtuel (équipement virtualisé), réseautique virtualisée (ex. : commutateur virtuel).

La mise en commun de *pools* de ressources physiques et virtuelles permet la virtualisation complète d'un environnement. Elle favorise la création de centres de traitement virtualisés.

Les possibilités de la virtualisation s'accompagnent d'une complexification tant sur le plan de l'exploitation que sur celui de la sécurité. Aux vulnérabilités du monde physique qui se transportent dans le virtuel s'ajoutent les vulnérabilités propres à la virtualisation. Les principaux enjeux de sécurité associés à la virtualisation sont les suivants :

- ✓ L'expertise limitée dans ce domaine;
- ✓ La méconnaissance des risques associés à la virtualisation;
- ✓ Le maintien de la séparation des tâches incompatibles;
- ✓ La gestion des privilèges d'administration (élevés);
- ✓ L'ajout d'une nouvelle surface d'attaque (hyperviseur).
- ✓ La gestion des incidents de sécurité des plateformes virtualisées;
- ✓ L'augmentation de la vulnérabilité aux menaces internes (malveillantes ou accidentelles);
- ✓ L'incapacité de s'assurer de la permanence du maintien des mesures de sécurité d'un environnement très dynamique;
- ✓ La difficulté de faire la preuve de la conformité (audit);
- ✓ La combinaison de plusieurs services sur un serveur, qui augmente les effets d'incidents de sécurité;
- ✓ Le partage d'informations entre les systèmes augmente la surface d'attaque;
- ✓ La difficulté d'identifier et de maintenir le périmètre de sécurité d'environnements très dynamiques;
- ✓ La sécurisation de tous les éléments de l'environnement;
- ✓ Le maintien de la sécurité de l'environnement.

Il est très difficile d'établir la portée et l'entendue des efforts de sécurité afin de déterminer le niveau de confiance à attribuer à ces environnements. Des efforts importants devront être consacrés afin de documenter et évaluer :

- ✓ L'ensemble des composantes de l'environnement virtuel déterminé par la portée de l'étude;

- ✓ Les vulnérabilités les plus fréquentes.

Une stratégie de défense en profondeur doit être adoptée et viser à :

- ✓ Sécuriser les couches technologiques;
- ✓ Isoler les fonctions de sécurité des fonctions applicatives;
- ✓ Évaluer l'hermétisme de l'hyperviseur : test, les rustines;
- ✓ Assurer que les fonctions de sécurité sont actives et supportées;
- ✓ Gérer de façon serrée les accès privilégiés (administrateur) par :
  - L'authentification à deux facteurs pour les administrateurs de l'infrastructure;
  - L'attribution du moindre privilège;
  - La journalisation et l'analyse de la journalisation des accès des comptes administrateurs.

Infonuagique

Le recours aux services d'infonuagique comporte de nombreux avantages, mais les OP n'en demeurent pas moins responsables d'assurer la disponibilité, l'intégrité et la confidentialité de l'information dont ils sont dépositaires. Par conséquent, les OP doivent être au fait des vulnérabilités de l'infonuagique sur le plan de la sécurité et veiller à ce que ces vulnérabilités soient atténuées, en accord avec les besoins des prestataires de services.

L'infonuagique est en mesure de fournir des services de TI adaptables, souples et abordables. Toutefois, une approche intégrée de la gestion des risques est à privilégier, comme il est énoncé dans la pratique recommandée. Différentes actions doivent être entreprises par les OP afin de déterminer les processus et les méthodes qui permettront de résoudre ces questions de façon à réduire les risques résiduels à un niveau acceptable par le détenteur de l'information ou le responsable de l'autorisation. Les principales actions à réaliser sont :

- ✓ Adopter le cadre de gestion en sécurité afin de mettre en place les processus de sécurité requis;
- ✓ Mettre en œuvre une méthode axée sur le cycle de vie de l'information pour évaluer et autoriser le recours à ce type de services;
- ✓ Préconiser une planification adéquate de l'architecture;
- ✓ Signer un accord sur les niveaux de service (ANS) officiel;
- ✓ Instaurer une gouvernance transparente et des contrôles et mesures de sécurité opérationnels efficaces;
- ✓ Évaluer les questions de sécurité associées aux services offerts par chacun des prestataires d'infonuagique.

De plus, il faut faire preuve de prudence dans le choix d'un prestataire de services d'infonuagique et mettre en place en place un processus de gestion des ententes afin d'examiner attentivement les aspects techniques et les clauses contractuelles qui ont trait à la sécurité.

Il y a deux façons complémentaires d'aborder les enjeux de sécurité associé à l'approvisionnement pour des services d'infonuagiques :

- ✓ Qualification : en incluant des exigences obligatoires ou cotées dans les critères d'évaluation qui rejettent à la présélection les technologies et les solutions de soumissionnaires non qualifiés[9];

9. En ce qui concerne un approvisionnement régi par un accord commercial, il faut veiller à ce que les critères d'évaluation soient entièrement divulgués et qu'ils soient conformes à l'accord commercial

- ✓ Contractualisation : en imposant des engagements contractuels aux fournisseurs qui procurent une certaine assurance d'intégrité, de disponibilité et de confidentialité de l'information externalisée et qui atténuent les menaces et les faiblesses associées aux services infonuagique acquis.

La rubrique suivante met en évidence certaines des considérations qui doivent être prises en compte pour réduire les risques de sécurité liés au recours à des prestataires d'infonuagique. Il importe :

- ✓ De demeurer à l'affût des lois régissant les infrastructures employées par les prestataires de services d'infonuagique et de s'assurer que lesdits prestataires sont à même de répondre à toutes les exigences de sécurité gouvernementale;
- ✓ De veiller à ce que les architectures d'infonuagique des clients soient intégrées afin d'assurer la prise en compte des incidents de TI. Les clients doivent effectuer des vérifications de sécurité des opérations ou de conformité à la réglementation. Par conséquent, ils doivent exiger que les prestataires de services d'infonuagique respectent les exigences en matière d'audit;
- ✓ D'intégrer au contrat, avant la migration, une stratégie de sortie qui prévoira la restitution des applications et des données du client ou les rediriger vers un autre prestataire; d'établir les critères qui pourront, le cas échéant, justifier l'application d'une telle stratégie (p. ex. : le prestataire cesse ses opérations ou ne respecte pas les dispositions du contrat ou de l'entente ou doutes concernant l'application des mesures de sécurité);
- ✓ D'établir des exigences, des règles portant sur la gestion de la chaîne d'approvisionnement des technologies, en établissant des lignes directrices sur l'élaboration de clauses d'acquisition.
- ✓ De conclure officiellement un accord sur les niveaux de service (ANS) couvrant les aspects énumérés ci-dessous :
  - Dispositions relatives au soutien des services TI;
  - Restrictions à l'égard de l'emplacement géographique des installations hôtes, des partenaires et des prestataires;
  - Restrictions relatives à la surveillance des activités et à la divulgation d'informations;
  - Clauses de résiliation en prévision de situations telles qu'une faillite du prestataire de services ou un changement de propriétaire;
  - Dispositions relatives aux services de continuité des activités et à l'intervention lors d'incidents de sécurité;
  - Dispositions relatives à la conservation et à la mise en lieu sûr des preuves numériques;
  - Dispositions relatives à la suppression sécurisée des données d'un dispositif mis hors service;
  - Processus sécurisé de sauvegarde des données;
  - Dispositions relatives à l'assurance de sécurité, à la conformité aux règlements et aux vérifications;
  - Dispositions relatives à la gestion de la sécurité, aux évaluations et aux autorisations de sécurité (EAS) ainsi qu'aux services consultatifs sur les vulnérabilités;
  - Avis et rapports;
  - Garanties de disponibilité assorties de sanctions en cas de non-conformité;
  - description claire des droits de propriété du prestataire de services en nuage et de ses relations avec des tierces parties;
  - Clause permettant d'effectuer régulièrement des vérifications de sécurité visant le prestataire de services d'infonuagique.

- ✓ De se doter d'une stratégie de mitigation des risques de sécurité prévoyant la sélection des normes et des audits exigés aux prestataires :
  - Le NIST (National Institute of Standards and Technology, É.-U.) et la Cloud Security Alliance fournissent des guides appropriés à ce sujet;
  - Les responsables de la sécurité interne doivent s'aligner sur les standards appropriés. Cet aspect doit être abordé avant la négociation d'ententes de service;
  - Le recours à des auditeurs externes pour la validation des mesures de sécurité est une approche à considérer.
- ✓ De déterminer les besoins en ce qui concerne la gestion de l'identité (selon les besoins d'affaires énoncés) entre le prestataire et l'organisme :
- ✓ De se référer aux orientations établies dans le cadre des travaux du Volet 1 – Orientations stratégiques et de la stratégie gouvernementale en matière d'authentification gouvernementale – Positionnement de l'authentification gouvernementale;
- ✓ D'adapter la politique de sécurité et le cadre de gestion, et de mettre à niveau l'architecture de sécurité de l'information en tenant compte des divers types de déploiement retenus;
- ✓ De prendre en considération les domaines de confiance dans l'élaboration des mesures prévues dans le cadre des travaux de développement de l'architecture d'entreprise gouvernementale;
- ✓ De mettre en place des processus et des mécanismes de reddition de comptes et d'évaluation concernant le respect des ententes, des exigences de la sécurité et de la qualité des services rendus aux citoyens et aux entreprises.

Mobilité et prenez vos appareils personnels[10] (PAP)

L'utilisation de dispositifs mobiles et de signaux sans fil met à risque les renseignements et les actifs informationnels du gouvernement du Québec. Il est impératif que les ministères du gouvernement du Québec mettent des mesures de sécurité en place afin d'assurer la protection, la disponibilité et l'intégrité de leurs renseignements et de leurs actifs liés aux informations.

Pour atténuer les risques que posent les dispositifs mobiles et signaux sans fil à l'égard de l'information sensible ou classifiée, les OP doivent adopter des pratiques de sécurité rigoureuses et aviser leurs employés des répercussions de leurs actions en matière de sécurité. Lorsqu'elles sont mises en œuvre ensemble, les mesures présentées ci-dessous peuvent réduire le risque de compromission de l'information. Les OP doivent :

- ✓ Mettre en place des politiques de sécurité solides, des programmes de formation et de sensibilisation, des mesures de sécurité adaptées et un processus rigoureux de gestion des risques afin d'accroître la sécurité de leurs réseaux et prévenir l'exfiltration de données;
- ✓ Élaborer des politiques et des règles internes claires sur l'utilisation de dispositifs sans fil dans les zones où sont traités des renseignements critiques ou classifiés, ou près de ces zones. Ces balises doivent servir d'éléments clés dans l'élaboration d'une stratégie globale de gestion des risques;
- ✓ S'assurer que les configurations de sécurité des solutions de gestion de dispositifs mobiles (*MDM* pour *Mobile Device Management*) sont clairement définies dans leurs politiques et procédures internes;
- ✓ Réaliser, sur une base régulière, des activités portant sur la sensibilisation aux vulnérabilités et sur l'adoption d'habitudes d'utilisation appropriées. Ces activités devraient être proposées à tous les utilisateurs ayant accès aux systèmes des OP.

10. En anglais, *Bring your own device* (BYOD).

En ce qui a trait au mode PAP, pour un organisme public :

- ✓ Se doter d'une vision et d'une stratégie architecturale globale en ce qui a trait à la mobilité (ex. : PAP, services éventuels à déployer dans l'infonuagique, applications pour les équipements mobiles, etc.), et ce, afin de protéger toutes les facettes de l'organisation;
- ✓ Déterminer comment le mode PAP est encadré au sein de son domaine de confiance (ex. : élaboration d'une directive spécifique, mise à jour du cadre de gestion de la sécurité, élaboration et mise à niveau de l'architecture de sécurité, etc.).

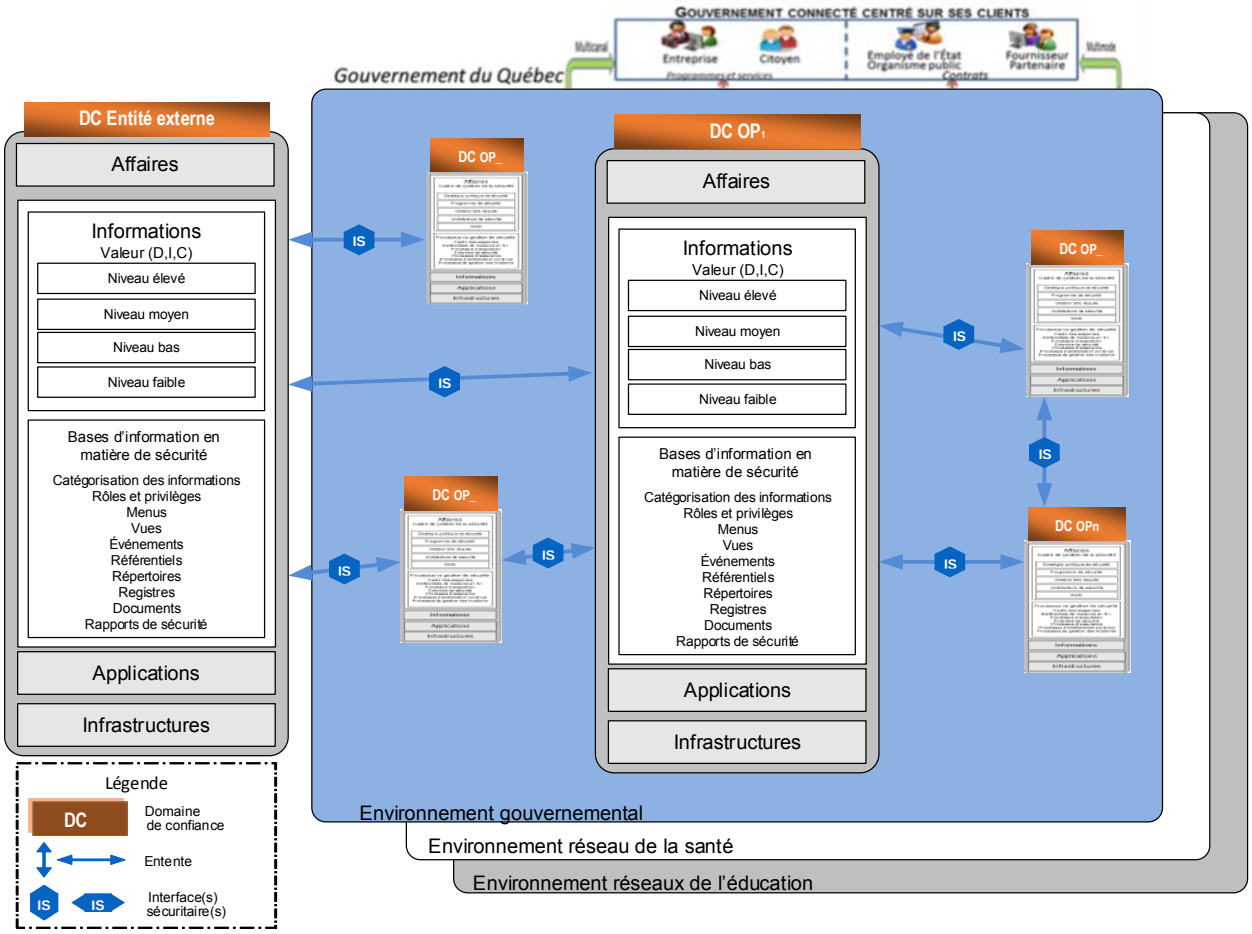
Collaboration sociale

Pour un organisme public désirant mettre en œuvre une plateforme collaborative dite sociale :

- ✓ Se doter d'une politique encadrant l'usage des médias sociaux et des modalités de collaboration sociale tant à l'interne qu'avec des partenaires externes;
- ✓ considérer les possibilités quant à la gouvernance inhérente à la collaboration sociale (ex. : mise en place de gestionnaires de communautés, notamment).

8.2 Volet « information »

Figure 7 : Vue « information »



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

La base d'informations en matière de sécurité est principalement constituée des informations relatives à la gestion des informations, 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. Parmi ce type d'informations, notons les certificats de clés publiques de chiffrement, les informations d'identification/authentification des entités, les profils d'habilitation/contrôle d'accès, les règles de surveillance, les règles de définition des virus, les règles de définition des accès des coupe-feu, les métadonnées en matière de sécurité, etc.

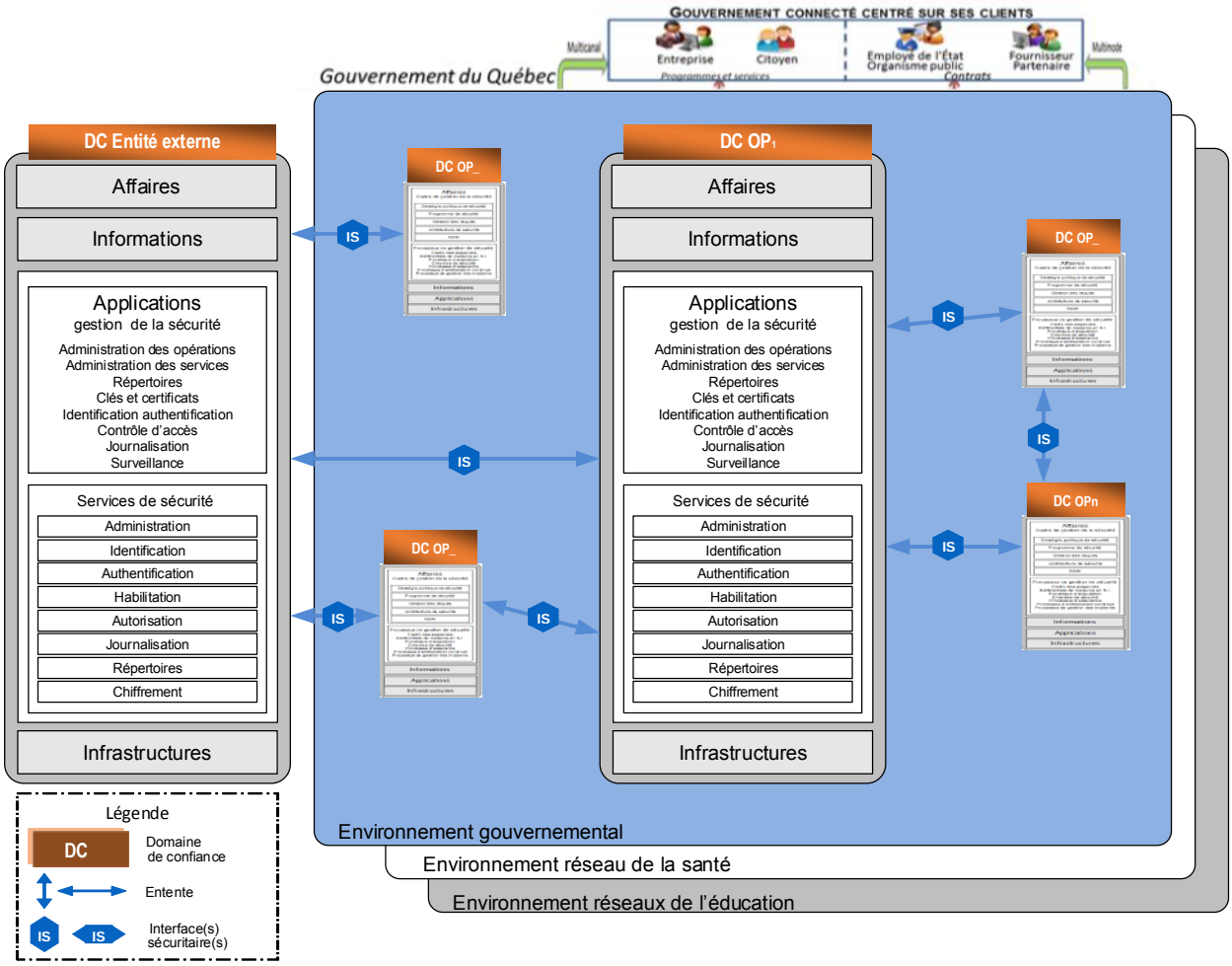
La base d'informations en matière de sécurité d'un domaine de confiance peut faire appel à des informations en matière de sécurité d'un ou de plusieurs autres domaines de confiance. Il faut donc accorder une attention particulière à la protection des échanges d'informations en matière de sécurité entre 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'informations entre les bases d'information en matière de sécurité sont nécessaires.

On peut identifier plusieurs éléments d'informations en matière de sécurité qui ont un potentiel de mise en commun, de partage ou de réutilisation. Ces potentiels devront être validés. À titre d'exemple :

- ✓ **Mise en commun :** répertoires gouvernementaux des informations relatives aux employés et aux partenaires/mandataires et certificats de clés publiques de chiffrement associés, base de données des informations relatives aux employés et aux partenaires/mandataires, base de données et fichiers des règles de sécurité du RITM.
- ✓ **Partage :** registre référentiel des schémas XML de sécurité normalisés, base de données et fichiers des règles de sécurité des secteurs de la santé et de l'éducation, registres référentiels particuliers XML des secteurs ou de grappes, bases de données des règles de sécurité des secteurs ou de grappes.
- ✓ **Réutilisation :** registres référentiels particuliers XML des OP, bases de données des règles de sécurité des OP, formulaires électroniques vierges.

8.3 Volet « application »

Figure 8 : Vue « application »



La base d'informations en matière de sécurité requiert une gestion adaptée à la valeur des informations qu'elle contient. À cet égard, chaque domaine de confiance doit mettre en place des applications relatives à la gestion de la sécurité. La base d'informations en matière de sécurité étant répartie, les domaines de confiance doivent sélectionner ou concevoir des produits facilitant une gestion centralisée des 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, autant si elles sont acquises que si elles sont conçues sur mesure. Dans l'éventualité où elles sont acquises, elles devront avoir fait leurs preuves dans l'industrie et être certifiées par des organismes reconnus, si pertinent.

Parmi ces applications, on retrouvera notamment celles assurant la gestion des répertoires, des clés et des certificats, de l'identification/authentification, de l'habilitation/contrôle d'accès, de l'administration (des logiciels et du matériel), des accès (unifiés), de la journalisation, de la surveillance, etc.

Les modules de sécurité visent à intégrer les fonctions de sécurité aux applications d'entreprise. Ils portent principalement sur l'identification/authentification, le chiffrement et le déchiffrement, l'intégrité, la signature et la vérification et la journalisation.

On peut cibler plusieurs applications (et modules) qui ont un potentiel de mise en commun, de partage ou de réutilisation. À titre d'exemple :

- ✓ **Mise en commun :** applications relatives à la gestion de la sécurité et les modules de sécurité (gestion du répertoire gouvernemental, gestion des clés et des certificats ICPG, gestion de l'administration, de la journalisation et de la surveillance du RITM, gestion de l'administration des applications gouvernementales et des serveurs gouvernementaux, modules d'identification et d'authentification, modules de chiffrement et de déchiffrement, etc.);
- ✓ **Partage :** applications relatives à la gestion de la sécurité et modules de sécurité dans les secteurs de la santé et de l'éducation et dans le secteur municipal (gestion de l'administration, de la journalisation et de la surveillance des réseaux sectoriels, modules d'identification et d'authentification, modules de chiffrement et de déchiffrement, etc.), applications et modules de sécurité propres à une grappe;
- ✓ **Réutilisation :** modules de sécurité propres à un OP (journalisation, vérification d'intégrité, etc.).

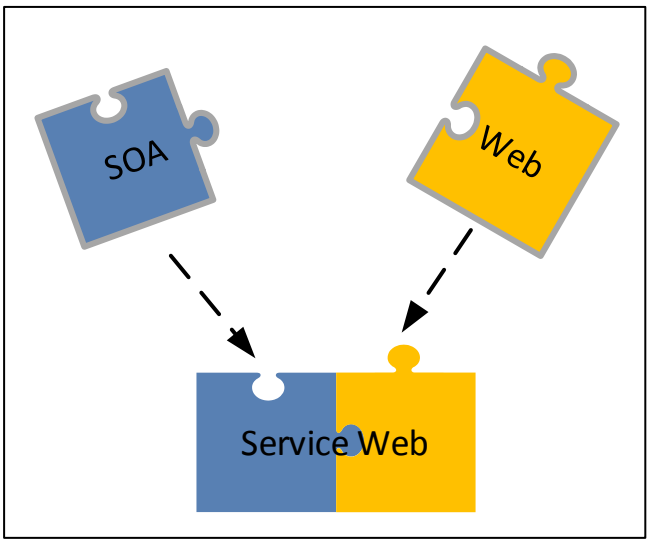
La prise en charge des enjeux de sécurité introduits par les architectures AOS et par l'infonuagique doit être considérée dans la constitution des domaines de confiance et lors de la négociation des ententes. Ainsi, il convient de considérer les enjeux engendrés par ces tendances dans la sélection des fonctions et des mécanismes de l'architecture de sécurité de l'information. Les considérations énumérées aux rubriques présentées ci-dessous sont en lien avec les sujets suivants.

AOS

L'architecture AOS est avant tout un modèle abstrait. En tant qu'architecture, elle s'attarde à la définition et à l'agencement des différentes composantes d'un système d'information en s'appuyant sur les processus d'affaires des organisations et sur la notion de services. Aucun standard ne lui est associé. Or, pour que les services soient interopérables, une normalisation est obligatoire. C'est sur ce plan que les services Web entrent en jeu.

La figure 9 illustre succinctement la relation qui existe entre l'architecture AOS et les services Web.

Figure 9 : De l'architecture AOS aux services Web



Les services Web sont, en quelque sorte, l'union des principes de l'architecture AOS et de l'environnement technologique du Web (HTTP, URI, XML, etc.). Ils offrent, grâce à leur éventail de standards, le cadre permettant la réalisation d'un modèle architectural orienté service (AOS). Le cadre commun d'interopérabilité du gouvernement du Québec énonce les standards de communication et de services soutenant et permettant la sécurisation des services élaborés selon cette approche architecturale.

De plus, l'apparition de ces standards n'est pas étrangère à ce repositionnement. Que ce soit XACML, SAML, XML Signature, XML Encryption, ou d'autres standards, il s'agit de fondements permettant de construire le nouveau modèle de sécurité. Dans le contexte, les défis de l'authentification et de la journalisation, de l'habilitation et le contrôle d'accès sont importants.

L'émergence de l'AOS assure l'agilité et la flexibilité dans la prestation de services, principalement par la réutilisation des fonctionnalités. Les cadres de développement basés sur les services Web permettent la création d'architectures distribuées. Par ce fait, les services Web ouvrent les systèmes, favorisant une meilleure agilité et favorisant l'intégration.

Une solution AOS typique est distribuée sur plusieurs domaines de sécurité et plusieurs identités peuvent être rattachées à un utilisateur, ce qui peut causer un problème à une approche traditionnelle de sécurité. Les infrastructures de sécurité peuvent varier d'un domaine à l'autre et obliger les utilisateurs à être identifiés à chaque domaine tandis qu'un service AOS à la couche composition peut appeler différents sous-services sous la juridiction de différents domaines de sécurité. Cependant, ces systèmes doivent être protégés contre les menaces tant internes qu'externes.

Du point de vue de l'architecture, les organisations ont des infrastructures en place pour protéger leurs actifs informationnels. Ces infrastructures devront prendre en compte les enjeux associés à l'AOS. Pour assurer la sécurité de bout en bout des services distribués, les OP devront ajouter une couche de plus à leur infrastructure de sécurité actuelle afin de protéger leurs actifs informationnels. Cette couche sera basée sur les standards des services Web. Pour qu'une AOS soit sécuritaire, elle doit prendre en compte les enjeux de sécurité suivants : la gestion des identités, le contrôle des politiques de sécurité distribuées, l'interopérabilité, la sécurité des messages et la confiance, plus précisément :

- ✓ En ce qui concerne les politiques de sécurité, une organisation peut vouloir que toute communication avec des services externes soit conforme aux politiques de sécurité qu'elle a établies. Les politiques déterminent les exigences, les mesures et les mécanismes. Par conséquent, les politiques doivent être validées lors de l'interaction et en fonction du contexte d'interaction;

- ✓ Lors des interactions entre composantes, basées sur les échanges de messages, les messages doivent rester confidentiels et non altérés, et leur origine, retraçable et non répudiable;
- ✓ Le « *loose coupling* » des services associés à l'AOS met explicitement la confiance à l'avant-plan et le besoin de déterminer des conditions assurant la confiance, en particulier l'identification des mesures et des mécanismes de sécurité requis;
- ✓ L'identité des services ou des dispositifs, ce qui nécessite l'authentification et l'autorisation des dispositifs à travers les différents domaines de confiance pour atteindre des objectifs de performance et de facilité d'utilisation, l'emploi de la fédération d'identités pour les environnements AOS;
- ✓ Le client et le service ne sont pas dans le même domaine de sécurité. Les politiques de sécurité doivent édicter les règles de sécurité tant des messages sortants (clients) qu'entrants (services).
- ✓ L'interopérabilité en sécurité doit reposer sur la notion de profil de sécurité de base;
- ✓ La confiance doit être établie avant que toute interaction soit autorisée.
- ✓ Les applications élaborées selon une AOS, à cause de leur ouverture et leurs interconnections requièrent des efforts importants afin d'assurer le développement d'applications sécurisées.
- ✓ Le domaine de confiance peut se découper en couches et suivre les interactions entre les sous-domaines ou les zones.
- ✓ La définition des niveaux de sécurité est importante et nécessite l'application du concept de zones de sécurité et influence la structure des mesures de sécurité et la combinaison optimale de mesures adéquates, car tout n'a pas à être au même niveau de sécurité.
- ✓ Les tests de la robustesse du concept.
- ✓ La détermination des principes guidant la définition du domaine de confiance pour une organisation.

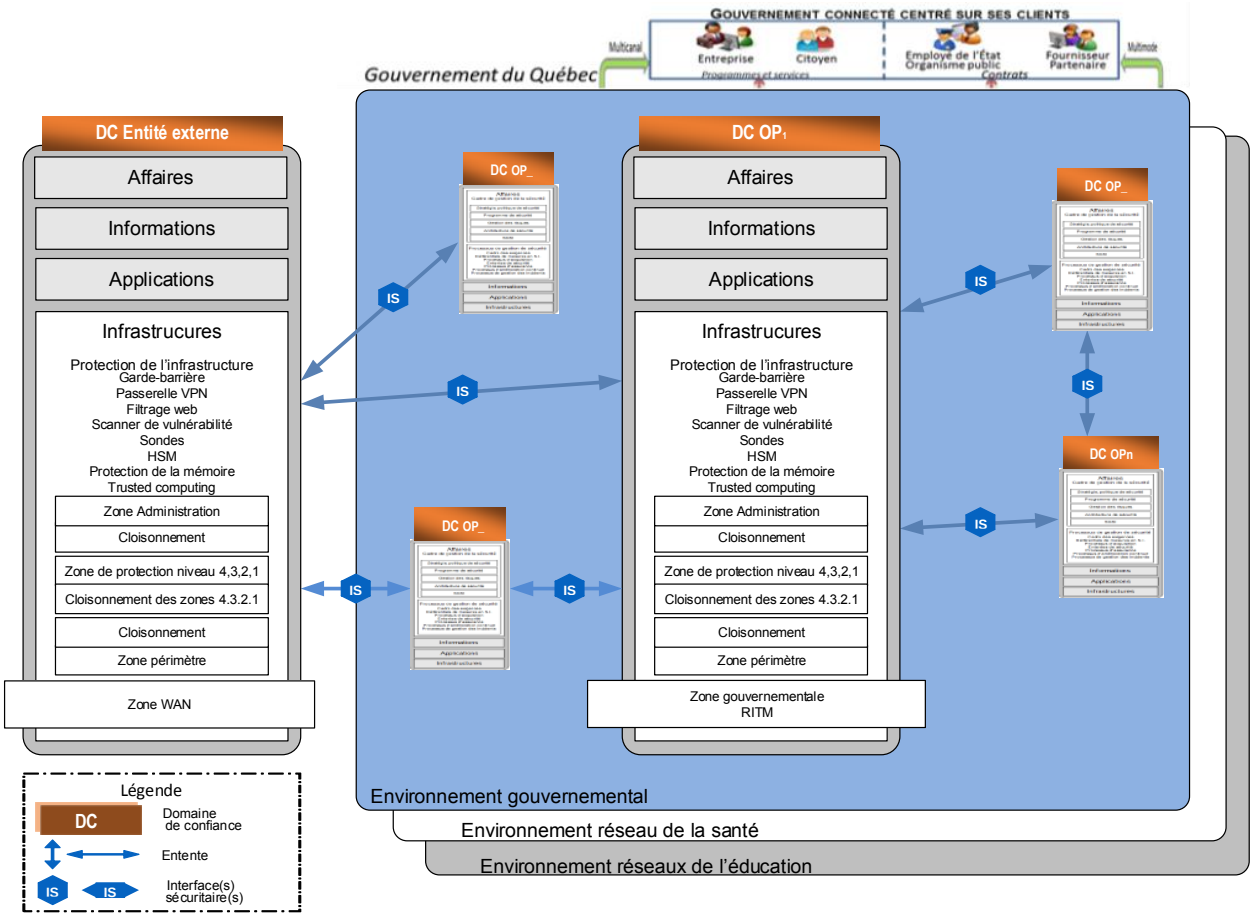
Infonuagique

Considérations de sécurité

- ✓ Mettre en place des moyens adéquats d'authentification et de contrôle d'accès avec autorisations axées sur les rôles pour les administrateurs des environnements hôte et invité;
- ✓ Utiliser des mécanismes adéquats d'authentification entre les composantes informatiques chargées du traitement de données sensibles;
- ✓ Maintenir et fournir une suite définie d'applications et d'API, préférablement au moyen d'une liste blanche;
- ✓ Imposer des accords de gestion visant les correctifs de logiciels et de systèmes d'exploitation, pour que lesdits correctifs soient installés en temps opportun;
- ✓ Surveiller les comptes réseau, afin de détecter les activités et les changements non autorisés et de produire des rapports réguliers.

8.4 Volet « infrastructure technologique »

Figure 10 : Vue « infrastructure technologique »



La figure 10 du volet « infrastructure technologique » introduit les concepts de cloisonnement et de zone. Le concept de cloisonnement permet le découpage en zones de manière à gérer adéquatement les accès. 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 ou les routeurs sont généralement utilisés pour protéger les zones.

Le découpage en zones facilite la protection des informations au niveau approprié. Chaque zone contient un ensemble d'équipements informatiques de réseautique et de logiciels regroupés en fonction de certaines considérations, telles que le type d'équipements et de logiciels, le type d'informations conservées, le type de services offerts et le type d'accès autorisés.

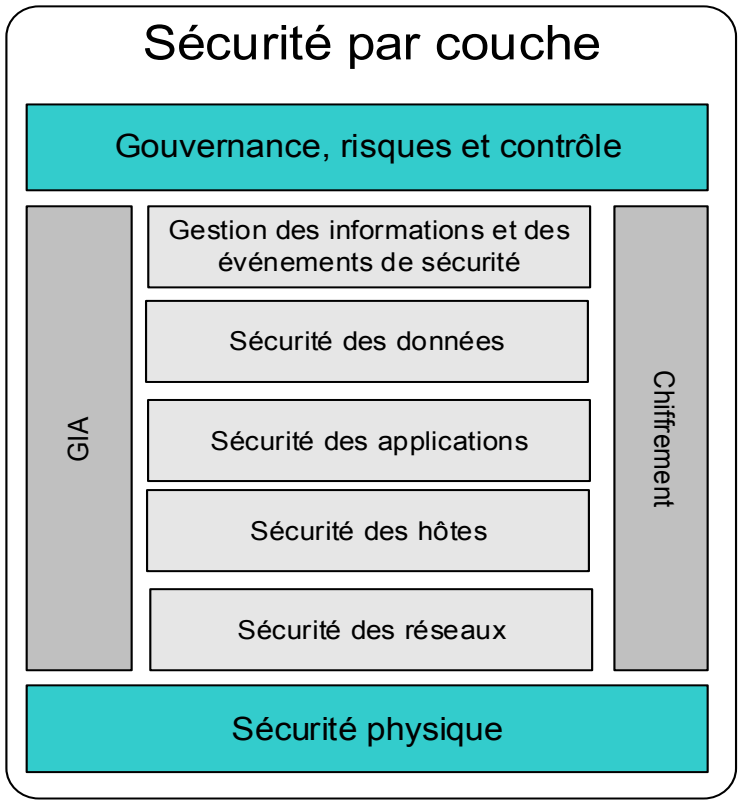
Les réseaux de transport permettent l'accès et l'échange des informations, y compris celles de la base d'information en matière de sécurité. En portant une attention particulière aux réseaux de transport, en particulier au RITM, on permettra de ne pas affaiblir la sécurité des domaines de confiance du périmètre gouvernemental.

Finalement, les interfaces sécuritaires du modèle utilisent les fonctions ou les mécanismes, fournis par les équipements et logiciels systèmes des zones et des cloisonnements afin de protéger de manière adéquate l'infrastructure. Ce volet introduit aussi le concept de sécurité par couche technologique. La figure 11 illustre cette approche qui est une composante de la sécurité en profondeur. Cette approche vise à identifier les interrelations entre les différentes couches technologiques d'une infrastructure ainsi que les fonctions et mécanismes de sécurité afin de protéger de façon adéquate l'infrastructure. Elle

réduit le risque qu'une faiblesse d'une partie soit exploitée de façon à ce que les mesures de protection des autres parties soient contournées. Voici les composantes de ce modèle de sécurisation :

- ✓ Sécurité réseau (filtre, coupe-feu, outils de sécurité réseau, DDOS, DNS, etc.);
- ✓ Sécurité des hôtes (gestion des correctifs, balayage des vulnérabilités, anti-maliciel, protection de la mémoire, gestions des configurations etc.);
- ✓ Sécurité des applications (balayage des applications, test d'intrusion, sondes, etc.);
- ✓ Sécurité des données (sécurité des bases de données, protection contre la fuite des données, etc.);
- ✓ Gestion de l'identité, des autorisations, des « privilèges », etc. ;
- ✓ Chiffrement (génération des clés, conservation des certificats, module de chiffrement matériel *Hardware Security Modul (HSM)*);
- ✓ Gestion des informations et des événements de sécurité (l'ensemble des outils qui organisent l'exploitation de l'information de sécurité générées par les autres couches : les journalisations, la corrélation, l'archivage).

Figure 11 : Modèle de sécurisation par couche



On peut identifier plusieurs éléments d'infrastructure technologique qui ont un potentiel de mise en commun ou de partage. À titre d'exemple :

- ✓ Mise en commun : solutions technologiques supportant les mécanismes de sécurité (serveurs du répertoire gouvernemental, serveurs de gestion des clés et des certificats, serveurs de détecteurs d'intrusions réseau et de virus du RITM, serveurs coupe-feu du RITM, serveurs de détecteurs des virus, serveurs coupe-feu de l'intranet gouvernemental, serveurs de contrôle d'accès (unifiés), détecteurs d'intrusions serveur, etc.

- ✓ Partage : serveurs du registre référentiel de schémas XML de sécurité normalisés, infrastructures technologiques en matière de sécurité des secteurs de la santé et de l'éducation (serveurs de détecteurs des intrusions réseau et de virus des réseaux sectoriels, analyseurs de vulnérabilité des réseaux sectoriels, serveurs coupe-feu des réseaux sectoriels, etc.), infrastructures technologiques en matière de sécurité propres à une grappe.

La prise en charge des enjeux de sécurité introduits par les architectures virtualisées, l'infonuagique et la mobilité doit être considérée lors de la sécurisation de l'infrastructure technologique. Les considérations énumérées aux rubriques proposées ci-dessous sont en lien avec les sujets suivants.

Environnement virtualisé

Du point de vue de la sécurité, la virtualisation ajoute à la complexité de gestion de la sécurité de ce type d'infrastructure. L'ajout de nouvelles couches technologiques, principalement de l'hyperviseur, ajoute les enjeux suivants :

- ✓ La création de multiples types de MV;
- ✓ La multiplication des profils de MV (utilisateurs, OS, applications, etc.);
- ✓ La mobilité des machines virtuelles (MV), qui peuvent se déplacer d'un serveur physique à l'autre, d'un environnement à l'autre;
- ✓ La visibilité limitée du trafic entre machines virtuelles;
- ✓ La perte d'information entre des segments de réseau virtuels;
- ✓ Les impacts de la sécurisation sur la performance technologique (sécurité par agent);
- ✓ L'exécution sur une unité physique de plusieurs MV de différents niveaux de confiance;
- ✓ L'immaturité des outils de supervision de l'exploitation et de la sécurité;
- ✓ L'inadaptation des outils de sécurité aux environnements virtuels (les outils d'analyse par balayage «*scanner*» notamment).

Les efforts de sécurité doivent porter sur l'adoption de pratiques en sécurité, la mise au point de processus d'exploitation ainsi que l'identification et utilisation des technologies de sécurité adaptées à la virtualisation. Il est recommandé, comme approche, de sécuriser l'hyperviseur de chaque hôte physique à l'aide d'un seul composant qui gère l'ensemble des requêtes de sécurité de l'hyperviseur. À cette pratique s'ajoutent les actions suivantes :

- ✓ La protection des MV dormantes;
- ✓ La protection des copies de MV et des images de MV;
- ✓ Le durcissement de l'hyperviseur, des machines virtuelles et des serveurs virtuels;
- ✓ La sécurisation de chaque MV par un agent;
- ✓ La journalisation et l'exploitation de la journalisation des échanges d'information;
- ✓ La gestion des mises à jour des correctifs;
- ✓ La gestion des configurations;
- ✓ La limitation et la protection des privilèges d'administration de la solution;
- ✓ La restriction de l'accès physique à l'environnement.

Infonuagique

- ✓ Employer des méthodes efficaces de sécurité du matériel et du personnel de façon à sécuriser l'infrastructure;
- ✓ Veiller à ce que les données inactives et les voies de communication soient sécurisées, conformément aux spécifications; les mécanismes de protection pourraient comprendre le chiffrement des données sortant de l'enclave gouvernementale;
- ✓ Utiliser des zones de sécurité pour isoler les serveurs et les données et activer ces zones par la mise en œuvre de coupe-feu et du filtrage des ports, établir des zones de sécurité dans un réseau.

Mobilité

Les OP devraient envisager d'adopter les mesures de sécurité suivantes pour sécuriser leurs dispositifs mobiles :

- ✓ Utiliser une liste blanche pour imposer des restrictions dans l'ensemble de l'organisme;
- ✓ Contrôler l'utilisation des caméras et des émetteurs sans fil;
- ✓ Restreindre les connexions à un réseau WiFi aux points d'accès autorisés du gouvernement du Québec.

8.5 Segment interopérabilité

La sécurité et la protection des renseignements personnels ou autrement confidentiels sont des obligations importantes pour les OP qui administrent des services publics. D'où la nécessité d'utiliser des normes et standards de sécurité adéquats et interopérables afin d'accroître l'efficacité et la cohérence des actions en la matière.

La sécurité a une portée transversale aux quatre volets mentionnés précédemment. Ainsi, au volet affaire, elle contribue à la définition des processus de collaboration entre les OP et leur partenaires afin d'atteindre les objectifs de sécurité fixés pour le service commun d'échange ou Web tout en prenant en compte les risques et les objectifs d'affaires. Au volet information, elle établit la définition précise des informations de sécurité (normalisation) associées aux processus, aux applications, aux activités de supervision et de reddition de compte. Au volet applicatif et infrastructure, elle vise l'identification des services, des mécanismes de sécurité afin d'assurer la sécurité des services d'échange ou Web sur les aspects techniques suivants : interfaces ouvertes, interconnexion, intégration des données, présentation et échange des données et accessibilité.

Des zones et des objets de normalisation potentiels ainsi que des normes ouvertes, de facto ou émergentes, pertinentes aux différents volets du modèle général de sécurité sont identifiées afin de fournir un guide et un cadre de référence aux intervenants en matière de sécurité au gouvernement du Québec. Il faut noter toutefois qu'un effort devra être fait par les OP pour l'adoption de cette normalisation afin d'assurer la nécessaire cohérence gouvernementale et se protéger contre les risques associés aux normes non reconnues.

Ces champs de normalisation potentiels (seuls les normes et standards dominants les plus pertinents sont indiqués) peuvent correspondre à des documents, des règles, des critères, des mécanismes de sécurité, des solutions technologiques ou des processus. Pour de plus amples informations sur ce sujet nous référons les lecteurs au document de l'AEG Cadre commun interopérabilité du Gouvernement du Québec version 2.0.

Finalement, il faut rappeler que le cadre normatif de sécurité du service d'échange ou Web à mettre en place sera influencé par le contexte des différentes parties prenantes. Au préalable, elles devront s'entendre sur les visions, les objectifs, les principes, les orientations et les niveaux de sécurité requis pour protéger les informations échangées.

ANNEXE I Lexique

Le tableau 6 décrit brièvement les termes propres à la sécurité utilisés dans le document.

Tableau 7 : Lexique des termes

Terme	Définition
Mesure de sécurité	Moyens de gestion des risques comprenant les politiques, les procédures, les lignes directrices, les pratiques ou l'organisation, qui peuvent être de nature administrative, technique, managériale ou juridique. (Source : ISO/CEI 27000:2009 – extrait du document de l'AFNOR de février 2011)
Objectif de sécurité	Déclaration décrivant ce qui doit être atteint comme résultat de la mise en œuvre des mesures de sécurité. (Source : ISO/CEI 27000:2009 – extrait du document de l'AFNOR de février 2011)
Programme de sécurité	Ensemble des éléments du système de gestion de la sécurité de l'information (SGSI) appuyé par un plan d'action pluriannuel (exemple : triennal, quinquennal) visant l'atteinte des objectifs (exemples : sectoriels, gouvernementaux) fixés en sécurité de l'information. (Source : inspiré des travaux de l'Office of Management and Budget américain)
Services de sécurité	Services nécessaires pour assurer la sécurité des informations. Ces services sont mis en place non seulement par des infrastructures et des applications appropriées, mais également grâce à une combinaison de mesures telles des structures organisationnelles et fonctionnelles, des processus, des informations de sécurité, etc. (Source : inspiré de COBIT 5, traduction libre)
Système de gestion	Cadre de référence composé de lignes directrices, de politiques, de directives, de processus, de procédures et de l'ensemble des ressources visant à assurer l'atteinte des objectifs d'une organisation. (Source : inspiré d'ISO/CEI 27000:2012)
Système de gestion de la sécurité de l'information (SGSI)	Portion du système de gestion visant l'établissement, la mise en œuvre, l'exploitation, la surveillance, le réexamen, la mise à jour et l'amélioration de la sécurité de l'information afin d'atteindre les objectifs fixés en la matière en se fondant sur l'appréciation des risques de l'organisation pour les traiter et les gérer efficacement. (Source : inspiré d'ISO/CEI 27000:2012)

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique