Sécurité

Cadre de référence de l'architecture de sécurité de l'information gouvernementale

Architecture d'entreprise gouvernementale 3.2

ENSEMBLE on fait avancer le Québec

Québec

Sécurité

Cadre de référence de l'architecture de sécurité de l'information gouvernementale

Architecture d’entreprise gouvernementale 3.2

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

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
2e étage, secteur 800
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 – janvier 2017
Bibliothèque et Archives nationales du Québec

ISBN (en ligne) 978-2-550-77522-5

Table des matières

Liste des figures

Liste des tableaux

Liste des sigles et acronymes

AEG	Architecture d’entreprise gouvernementale
AOS	Approche orientée services
ASIG	Architecture de sécurité de l’information gouvernementale
COMSI	Communauté de sécurité de l'information
DPI	Dirigeant principal de l'information
IAAS	*Infrastructure as a service* (services d'infrastructure)
IOS	Infrastructure orientée services
LGGRI	Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement
PAAS	*Platform as a service* (services de plateforme)
PES	Prestation électronique de services
REVSI	Réseau d'experts et de vigie en sécurité de l'information
SAAS	*Software as a service* (services d'applications ou de logiciels)
SCT	Secrétariat du Conseil du trésor
SI	Sécurité de l'information
TIC	Technologies de l’information et des communications

Historique des changements

Version de l'AEG	Statut	Modifications
3.2	Juin 2016	Publication de la première édition

La version en vigueur est disponible à l'adresse suivante :

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

Avis aux lecteurs

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 du réseau 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 document soient applicables à la plupart des organismes publics, il convient d'adapter chacun d'entre eux à son contexte et aux risques qui lui sont propres.

Public cible

- ✓ Responsables organisationnels de la sécurité de l'information (ROSI)
- ✓ Conseillers organisationnels de la sécurité de l'information (COSI)
- ✓ Architectes de sécurité de l'information
- ✓ Spécialistes en sécurité de l'information
- ✓ Responsables des technologies de l'information
- ✓ Architectes d'entreprise
- ✓ Gestionnaires

Introduction

Les technologies de l'information représentent un puissant levier de rénovation de l'État. Elles jouent un rôle central dans la gestion rigoureuse des dépenses de l'État et l'amélioration de la prestation des services aux citoyens et aux entreprises. Leur développement accéléré ainsi que l'utilisation croissante d'Internet ont considérablement modifié les règles d'échange et de partage de l'information.

Ainsi, l'Administration gouvernementale s'est dotée en 2015 d'une véritable stratégie en technologies de l'information, la Stratégie gouvernementale en TI : Rénover l'État par les technologies de l'information. Cette stratégie tient compte, pour sa mise en œuvre, de l'apport incontournable de la sécurité de l'information, particulièrement en ce qui a trait au renforcement de la gouvernance, à la gestion des talents, à l'adoption des meilleures pratiques et au rapprochement de l'État des citoyens.

Pour concrétiser la mise en œuvre de la Stratégie gouvernementale en TI, l'architecture d'entreprise gouvernementale (AEG) définit les orientations stratégiques gouvernementales en matière de ressources informationnelles. Ainsi, le présent document vise à déterminer les fondations nécessaires pour sécuriser l'information gouvernementale tout en restant aligné sur ces orientations. Ces fondations constituent l'essence même de l'architecture de sécurité de l'information gouvernementale. Elles en précisent les exigences, les principes, la vision, les orientations stratégiques et les lignes directrices pour les volets Affaires, Information, Applications et Infrastructures de l'AEG.

1. Qu'est-ce qu'une architecture de sécurité de l'information ?

La norme ISO/IEC 42010:/2007 définit l'architecture comme étant « l'organisation fondamentale d'un système, mise en œuvre par ses composants, par les relations que ces derniers ont entre eux et avec l'environnement et par les principes qui en régissent la conception et l'évolution ».

Le TOGAF[1] reprend et élargit cette définition en précisant que, selon le contexte d'utilisation, l'architecture a une double signification :

- ✓ l'architecture est une description formelle d'un système ou un plan détaillé des composantes du système pour guider sa mise en œuvre;
- ✓ l'architecture est la structure des composantes, leurs interrelations et les principes et guides gouvernant leur conception et leur évolution dans le temps.

En matière de sécurité, le TOGAF précise que « pour être effective, la sécurité doit être forte, jamais tenue pour acquise et elle doit être désignée à l'intérieur d'une architecture et jamais attachée à elle par la suite ». En plus, « dans le but d'établir une architecture de sécurité, la meilleure approche consiste à considérer ce qui est à protéger, quelle est sa valeur et quelles sont les menaces ».

Selon l'entreprise Gartner[2], l'architecture de sécurité de l'information est un processus continu de planification stratégique qui vise à assurer la cohérence et l'alignement des composantes d'un programme de gestion de la sécurité de l'information avec les orientations d'affaires. À cet égard, Gartner définit l'architecture de sécurité comme étant un processus qui délivre la documentation de planification, de conception et d'implémentation en soutien au programme de gestion de la sécurité de l'information.

À partir de ce qui précède, nous définissons ASIG comme étant « un cadre de référence qui circonscrit les préoccupations gouvernementales en sécurité de l'information alignées sur les orientations stratégiques fixées dans l'architecture d'entreprise gouvernementale, qui définit la vision et les orientations gouvernementales en matière de sécurité de l'information et identifie les éléments d'encadrement pour la prise en charge des exigences de sécurité de l'information gouvernementale ».

2. Contexte légal, administratif et normatif

Dans sa démarche de transformation de la prestation de services aux citoyens et aux entreprises, le gouvernement du Québec a placé la sécurité de l'information au cœur de ses priorités. En effet, l'utilisation croissante d'information de toute nature sur les citoyens, les entreprises et les organismes publics soulève des enjeux de disponibilité de cette information, des questionnements sur son intégrité et sa confidentialité, lesquels appellent la mise en place d'un encadrement légal, administratif et normatif de la gestion de la sécurité de l'information et un soutien continu des organismes publics dans la prise en charge des exigences en matière de sécurité de l'information.

C'est ainsi que la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI), adoptée en juin 2011, a introduit des dispositions en

1. TOGAF : The Open Group Architecture Framework
2. Gartner : entreprise de conseils et de recherches dans le domaine des techniques avancées.

ce qui a trait à l'établissement de règles de sécurité de l'information et au suivi de leur mise en œuvre, tant sur le plan gouvernemental que sectoriel[3].

Quant à la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics, déposée à l'Assemblée nationale en 2010 et actualisée en 2012, elle reconnaît l'importance de la sécurité de l'information en tant qu'élément clé permettant d'assurer la pérennité du patrimoine informationnel gouvernemental. À cet égard, elle énonce les orientations gouvernementales et met l'accent sur les actions visant à faire face aux enjeux de sécurité de l'information de l'heure.

De plus, un nouveau cadre de gouvernance de la sécurité de l'information gouvernementale a été adopté en janvier 2014. Formalisé au moyen de quatre documents[4], ce cadre vise à instaurer une gouvernance forte et intégrée de la sécurité de l'information et à concrétiser la vision gouvernementale en la matière.

Sur le plan normatif, l'émergence de plusieurs tendances en technologies de l'information telles que l'infonuagique, la mobilité, les données ouvertes (libération des données) ou la collaboration sociale a donné lieu à l'évolution des normes et standards en matière de sécurité de l'information : la norme ISO 27018 qui porte sur l'infonuagique et la protection des renseignements personnels ou la norme ISO 27017 qui porte sur les contrôles de sécurité dans les services infonuagiques.

3. Objectifs et portée de l'architecture de sécurité de l'information gouvernementale

3.1 Objectifs

L'ASIG a pour objectif d'identifier les éléments d'encadrement de haut niveau permettant de promouvoir auprès des organismes publics une vision commune de la sécurité de l'information, alignée sur l'AEG. Cette vision contribue à la cohérence des actions en vue d'assurer une protection adéquate de l'information gouvernementale et, ainsi, de rehausser la confiance des citoyens et des entreprises à l'égard de l'État. Elle soutient l'ensemble des composantes (Affaires, Information, Applications et Infrastructures) de l'AEG et permet d'organiser la transformation progressive et continue de la sécurité de l'information gouvernementale.

Ainsi, l'ASIG est un outil pour mieux piloter et gouverner la sécurité de l'information et alimenter efficacement le plan stratégique gouvernemental en cette matière. L'objectif de ce plan est d'assurer la mise en place de mesures de sécurité de l'information de qualité proportionnelle à la valeur de l'information gouvernementale à protéger et aux risques de sécurité de l'information courus par les ministères et organismes.

3. Sectoriel : c'est-à-dire de portée ministérielle.

4. Directive sur la sécurité de l'information gouvernementale adoptée depuis janvier 2014; Cadre gouvernemental de gestion de la sécurité de l'information; Approche stratégique gouvernementale 2014-2017 en sécurité de l'information; Cadre de gestion des risques et des incidents à portée gouvernementale.

L'ASIG sert également de référence aux organismes publics pour la conception et la mise en œuvre d'une architecture de sécurité de l'information propre à leur organisation (architecture de sécurité de l'information sectorielle [5]), alignée sur la vision gouvernementale et qui serait à la base de toute initiative de développement et de mise en œuvre d'un programme adéquat de gestion de la sécurité de l'information. Les architectures de sécurité de l'information sectorielles ainsi conçues constitueront la pierre angulaire du programme gouvernemental de sécurité de l'information.

3.2 Portée

L'ASIG est appelée à progresser selon le processus itératif d'évolution de l'AEG afin de maintenir la capacité de l'Administration gouvernementale à protéger l'information qu'elle détient, tout au long de son cycle de vie et quel que soit son support (support papier, numérique ou autre) ou son moyen de communication (communication électronique ou autre). L'information visée est celle qu'un organisme public détient dans l'exercice de ses fonctions, que sa conservation soit assurée par lui-même ou par un tiers.

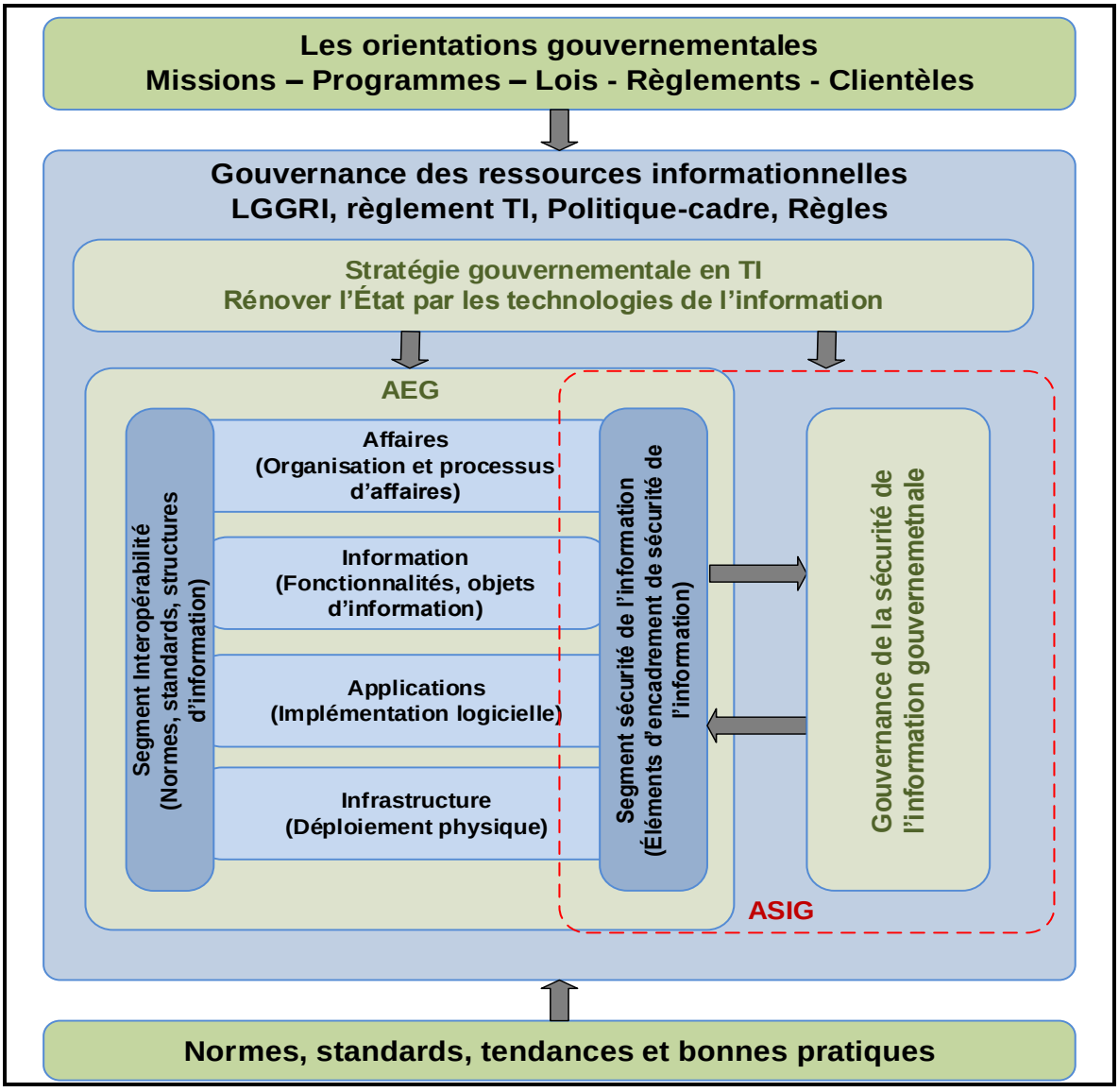
5. L'architecture de sécurité de l'information sectorielle est un outil stratégique qui définit la vision et les orientations en sécurité de l'information de l'organisme public. Elle est alignée sur les orientations gouvernementales et tient compte des objectifs d'affaires de l'organisation et des risques de sécurité de l'information associés. Elle permet de circonscrire les préoccupations de l'organisation en matière de disponibilité, d'intégrité et de confidentialité de l'information et, ainsi, de contribuer à l'élaboration et à la mise en œuvre d'un programme (plan directeur) de sécurité de l'information cohérent et intégré.

Note : L'architecture de sécurité de l'information sectorielle est élaborée selon un processus itératif qui tient compte de l'évolution de l'architecture d'entreprise. Elle est idéalement articulée autour des volets Affaires, Information, Applications et Infrastructures de l'architecture d'entreprise, lesquels intègrent, mais ne s'y limitent pas, les préoccupations relatives au partage sécuritaire de l'information, à la protection de l'accès à l'information, à la sécurisation des réseaux et des infrastructures, à la sécurisation des applications et des systèmes d'information, à la continuité des affaires et à la journalisation des opérations.

4. Modèle de l'architecture de sécurité de l'information gouvernementale

La figure suivante illustre la position de l'ASIG dans le contexte gouvernemental de la gouvernance des ressources informationnelles.

Figure 1 : Modèle d'ASIG



Conformément à la figure 1, la gouvernance des ressources informationnelles est régie par les orientations gouvernementales en matière de programmes, missions, lois et règlements, et plus précisément par la LGGRI, la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics et la Stratégie gouvernementale en TI. En prenant appui sur ces éléments et les normes, standards, tendances et bonnes pratiques en matière de gestion des ressources informationnelles,

l'AEG définit ses orientations stratégiques selon quatre volets : Affaires, Information, Applications et Infrastructures. Les préoccupations de ces volets en matière d'interopérabilité et de sécurité de l'information sont représentées par les segments transversaux (Interopérabilité et Sécurité).

Le segment Sécurité précise les différentes préoccupations relatives à la sécurité de l'information engendrées par les orientations fixées dans chacun des volets, il définit les objectifs de sécurité de l'information à atteindre pour en assurer la prise en charge et énonce les lignes directrices de sécurité de l'information pour chacun des volets.

Par ailleurs, la gouvernance de la sécurité de l'information est élaborée en prenant appui sur les éléments de contexte de la gouvernance des ressources informationnelles et des normes, standards et bonnes pratiques en matière de sécurité de l'information et elle offre un cadre structurant au segment Sécurité.

Ainsi, l'ASIG de haut niveau intègre deux composantes principales :

- ✓ la gouvernance de la sécurité de l'information gouvernementale;
- ✓ le segment Sécurité de l'AEG.

Le détail de ces composantes est présenté dans ce qui suit.

4.1 Gouvernance de la sécurité de l'information

La composante « Gouvernance de la sécurité de l'information » de l'ASIG est constituée de plusieurs éléments qui se déclinent comme suit :

- ✓ Principes généraux de la sécurité de l'information;
- ✓ Vision de la sécurité de l'information gouvernementale;
- ✓ Orientations gouvernementales en matière de sécurité de l'information;
- ✓ Cadre de gouvernance de la sécurité de l'information gouvernementale.

4.1.1 Principes généraux de la sécurité de l'information

La sécurité de l'information gouvernementale est régie par les principes suivants :

- ✓ **Vision commune :** l'atteinte d'un niveau de sécurité de l'information adéquat nécessite l'adhésion à une vision et une compréhension communes de la sécurité au sein des organismes publics et au plan de la coordination des actions gouvernementales.
- ✓ **Cohérence :** la sécurité de l'information repose sur une approche globale et intégrée qui tient compte des aspects humains, organisationnels, physiques, techniques et juridiques et nécessite la mise en place d'un ensemble de mesures coordonnées de prévention, de détection et de correction.
- ✓ **Accessibilité :** les services gouvernementaux doivent être facilement accessibles, conviviaux et sécuritaires, quels que soient les préférences de la clientèle gouvernementale, ses capacités et ses choix naturels.
- ✓ **Proportionnalité :** les mesures de sécurité de l'information sont établies en fonction de la sensibilité de l'information et doivent être proportionnelles aux risques courus. Ainsi, la gestion de la sécurité de l'information doit être fondée sur la prise en charge des risques relatifs à la sécurité de l'information.
- ✓ **Responsabilité et obligation redditionnelle :** l'efficacité des mesures de sécurité de l'information exige l'attribution claire de responsabilités à tous les niveaux de l'organisation et la mise en place

d'un processus de gestion interne de la sécurité de l'information permettant une reddition de comptes adéquate.

- ✓ **Évolution :** toute démarche de sécurité de l'information doit s'inscrire dans un processus d'amélioration continue. À cet égard, les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux ainsi que de l'évolution des menaces et des risques relatifs à la sécurité de l'information.
- ✓ **Universalité :** les pratiques et les solutions retenues en matière de sécurité de l'information doivent correspondre, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées à l'échelle nationale et internationale.
- ✓ **Éthique :** le processus de gestion de la sécurité de l'information doit être soutenu par une démarche d'éthique visant à assurer la régulation de la conduite des personnes et la responsabilisation individuelle.
- ✓ **Confiance :** la consolidation de la confiance des citoyens et des entreprises doit être au cœur des préoccupations gouvernementales en matière de sécurité de l'information.

4.1.2 Vision de la sécurité de l'information gouvernementale

La vision de la sécurité de l'information gouvernementale, sur un horizon de dix ans, se précise 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 mis en œuvre. Tout risque de sécurité de l'information est géré en tenant compte des répercussions sur l'ensemble du gouvernement. »

4.1.3 Orientations gouvernementales en sécurité de l'information

Les orientations stratégiques pour concrétiser la vision gouvernementale en sécurité de l'information tiennent compte de l'actuel contexte gouvernemental en matière de gestion des ressources informationnelles. Elles se déclinent comme suit :

Renforcer l'encadrement de la sécurité de l'information

Le renforcement de l'encadrement de la sécurité de l'information est déterminant pour assurer la cohérence et la coordination des interventions en cette matière à tous les niveaux de l'Administration gouvernementale. Il passe nécessairement par la définition et la mise en place de cadres de gouvernance de la sécurité de l'information, articulés autour de l'intégration et de la réutilisation des services. Ces cadres de gouvernance doivent tenir compte des orientations de l'AEG, notamment la mise en place d'une approche orientée services, le choix de solutions infonuagiques, le déploiement de sources officielles d'information ou le partage d'infrastructures communes.

Atteindre un niveau de maturité adéquat en sécurité de l'information

Un niveau de maturité convenable en sécurité de l'information est atteint lorsque les processus de sécurité de l'information et de protection des renseignements personnels et de la vie privée sont normalisés, intégrés, documentés et mis en œuvre et lorsque l'information gouvernementale est sécurisée, conformément aux meilleures pratiques de sécurité de l'information et en tenant compte des menaces qui pèsent sur celle-ci.

Assurer la sécurité des services communs et partageables

Les services communs et partageables sont sécurisés, notamment, lorsque la disponibilité, l'intégrité et la confidentialité de l'information sont assurées, les échanges entre les usagers et la plateforme gouvernementale sont sécurisés, le cadre de gestion des risques en sécurité de l'information des infrastructures communes est défini et les exigences pour assurer une interopérabilité sécuritaire entre les composantes de l'environnement gouvernemental sont reconnues.

Les services communs et partageables sont également sécurisés lorsque les mesures permettant d'instaurer la confiance entre les différentes parties prenantes d'une approche orientée services (AOS) sont mises en œuvre et les pratiques exemplaires d'intégration de la sécurité de l'information, des contrôles et de la protection des renseignements personnels sont élaborées en soutien au développement d'applications autour de solutions partageables.

Adopter une approche de sécurisation de l'information adaptée aux technologies émergentes et aux nouvelles tendances en technologies de l'information

Cette orientation se concrétise lorsque, notamment :

- ✓ la gestion des risques et des incidents de sécurité de l'information prend en charge les technologies émergentes;
- ✓ le choix, par les organismes publics, de solutions infonuagiques et d'environnements virtualisés est appuyé par un encadrement de sécurité de l'information;
- ✓ le niveau de maturité en sécurité de l'information des logiciels libres consignés dans le « catalogue gouvernemental des logiciels libres » est évalué et intégré; de plus, les critères d'évaluation sont documentés;
- ✓ les pratiques exemplaires d'encadrement des organismes publics dans le processus de libération de données sont élaborées en vue de garantir le respect de la vie privée et la protection des renseignements personnels;
- ✓ un encadrement de sécurité de l'information dans un contexte de mobilité et de collaboration sociale est élaboré et mis en œuvre.

4.1.4 Cadre de gouvernance de la sécurité de l'information gouvernementale

Le Sous-secrétariat du dirigeant principal de l'information a élaboré un cadre de gouvernance de la sécurité de l'information gouvernementale afin d'assurer la sécurité de l'information ainsi que pour maintenir et rehausser la confiance des citoyens et des entreprises à l'égard de l'État et des services publics. Ce cadre repose sur quatre documents :

- ✓ La « Directive sur la sécurité de l'information gouvernementale », adoptée en janvier 2014, a pour objet de garantir la sécurité de l'information qu'un organisme public détient et collecte dans l'exercice de ses fonctions, que la conservation de cette information soit assurée par lui-même ou par un tiers. Elle fixe les objectifs à atteindre et établit les obligations du dirigeant principal de l'information et des organismes publics pour assurer la sécurité de l'information gouvernementale tout au long de son cycle de vie.
- ✓ Le « Cadre gouvernemental de gestion de la sécurité de l'information » complète les dispositions énoncées à la « Directive sur la sécurité de l'information gouvernementale » en précisant l'organisation fonctionnelle de la sécurité de l'information au gouvernement du Québec ainsi que les rôles et responsabilités sur les plans gouvernemental et sectoriel.
- ✓ L'« Approche stratégique gouvernementale 2014-2017 en sécurité de l'information gouvernementale » définit la mission du gouvernement du Québec en matière de sécurité de

l'information et détermine les éléments essentiels à la réalisation de son encadrement. Elle fixe les cibles gouvernementales à atteindre en la matière pour les trois prochaines années et définit les indicateurs gouvernementaux de suivi du degré d'atteinte de ces cibles.

- ✓ Le « Cadre de gestion des risques et des incidents à portée gouvernementale » présente une approche novatrice de gestion des risques et des incidents susceptibles de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale.

4.2 Segment Sécurité

Le segment Sécurité de l'AEG évalue les risques de sécurité de l'information associés aux orientations stratégiques de l'AEG, définit les objectifs de sécurité de l'information requis pour en atténuer les impacts et énonce les lignes directrices de sécurité de l'information gouvernementale particuliers aux volets Affaires, Information, Applications et Infrastructures.

4.2.1 Préoccupations de sécurité de l'information en soutien aux orientations de l'architecture cible de l'AEG

La transformation gouvernementale ciblée par les orientations de l'architecture cible de l'AEG engendre de nouveaux risques en matière de sécurité de l'information gouvernementale, notamment ceux associés à une prestation gouvernementale faisant intervenir plusieurs parties prenantes, à l'utilisation d'une identification gouvernementale unique pour accéder à l'ensemble des services de l'État, aux différentes interactions qui existent entre les clientèles et les organismes publics ainsi qu'entre les organismes publics pour le partage des services et enfin ceux relatifs aux infrastructures ou aux échanges d'information sensible.

En vue d'une prise en charge adéquate de la sécurité de l'information gouvernementale en soutien aux orientations de l'architecture cible de l'AEG, il est important de déterminer les objectifs de sécurité de l'information à atteindre. Le tableau synthèse se trouve à la page suivante.

Tableau 1 : synthèse

Orientations de l'AEG 3.2	Objectifs de sécurité de l'information
Approche orientée services (AOS)	▪ Assurer la prise en charge de la sécurité de l'information dans le cadre d'une approche orientée services ▪ Déterminer les mesures de sécurité de l'information qui permettront d'instaurer la confiance entre les différentes parties prenantes d'une solution AOS
Fédération de l'information	▪ Prendre en charge les risques en matière de sécurité associés à l'information fédérée afin d'assurer la disponibilité, l'intégrité et la confidentialité de l'information fédérée
Le gouvernement comme une plateforme	▪ Offrir une plateforme gouvernementale sécuritaire
Infonuagique	▪ Encadrer les organismes publics dans le choix de solutions infonuagiques sécuritaires
Sources officielles d'information	▪ Définir un cadre de gouvernance en sécurité de l'information des sources officielles d'information
Logiciel libre	▪ Définir les critères d'évaluation de la maturité des logiciels libres en matière de sécurité de l'information ▪ Encadrer les communautés qui développent des solutions partageables en matière de sécurité de l'information
Gouvernement ouvert	▪ S'assurer du respect de la protection des renseignements personnels et de la vie privée dans un contexte de libération de données
Mobilité et BYOD	▪ Assurer la sécurité de l'information de l'organisme dans un contexte de mobilité des employés ▪ Sensibiliser les utilisateurs de terminaux mobiles à la protection de l'information à l'égard de toute tentative d'indiscrétion
Web participatif et collaboratif (collaboration sociale)	▪ Déterminer les règles de gouvernance de la sécurité de l'information en matière de collaboration sociale
Mise en place des infrastructures communes	▪ Définir un cadre de gestion des risques en matière de sécurité de l'information associés aux infrastructures communes
Interopérabilité	▪ Déterminer les exigences visant à assurer une interopérabilité sécuritaire entre les services gouvernementaux

Approche orientée services (AOS)

L'AOS est un paradigme favorisant la réutilisation et le partage des composantes. Elle permet d'organiser et d'utiliser des fonctionnalités distribuées, c'est-à-dire des services qui sont sous la responsabilité de différents propriétaires de domaines d'affaires et qui sont agencés pour répondre à un besoin déterminé. Cette approche constitue un levier efficace d'optimisation des ressources, puisqu'un même service peut être partagé et réutilisé.

L'AOS permet de construire des systèmes d'information évolutifs, modulaires et aptes à favoriser la réutilisation et le partage des composantes. Elle assure la flexibilité, l'agilité et l'efficacité de l'organisation et permet d'améliorer sa capacité de travailler avec différents acteurs (intervenants, partenaires, fournisseurs et clients).

Lorsqu'elle s'appuie sur les normes et les standards ouverts appropriés, l'AOS accroît l'interopérabilité entre les systèmes, les branches d'affaires et les organismes publics. Cette approche permet au gouvernement d'évoluer vers de nouvelles infrastructures partagées et consolidées.

Objectifs de sécurité de l'information

- ✓ Assurer la prise en charge de la sécurité de l'information dans le cadre d'une AOS

  Les organismes ne peuvent plus gérer la sécurité à l'échelle exclusivement applicative et doivent plutôt se concentrer sur des solutions interorganisationnelles qui s'articulent autour de l'intégration et de la réutilisation des services partagés. Ainsi, il y a lieu d'encadrer les organismes publics pour repenser la sécurité selon cette nouvelle perspective. Pour ce faire, il importe, notamment :

  - d'encadrer les organismes publics dans la mise en place d'une AOS;
  - de convenir des services de sécurité de l'information à mettre en commun au niveau gouvernemental;
  - de préciser les normes et standards à appliquer pour développer des services de sécurité interopérables;
  - d'analyser les risques en sécurité de l'information associés à la localisation d'un catalogue des services partageables pour s'assurer de la disponibilité, de l'intégrité et de la confidentialité de l'information gouvernementale.

- ✓ Déterminer les mesures de sécurité de l'information qui permettront d'instaurer la confiance entre les différentes parties prenantes d'une solution AOS

  Une solution AOS peut être distribuée et un service peut se composer de sous-services relevant de différentes organisations. Le faible couplage des services associés à une architecture de type AOS met à l'avant-plan la notion de confiance à l'égard des partenaires. À cet effet, il est important de considérer les préoccupations de sécurité suivantes :

  - identifier adéquatement le prestataire, le partenaire ou le consommateur du service;
  - définir et exposer les droits d'accès à un service;
  - assurer la confidentialité des échanges d'information;
  - assurer la conservation des messages lors d'un échange d'information sensible mettant en jeu plusieurs partenaires et définir les responsabilités de chacun des participants;
  - désigner une autorité responsable à l'égard de la définition des mesures de sécurité de l'information lorsque des renseignements sont partagés par plusieurs partenaires;
  - définir les exigences de sécurité d'un service pour éviter qu'il soit le maillon faible de la chaîne des composantes d'un autre service (préciser les failles de sécurité potentielles d'un service);
  - sécuriser les interfaces des services développés;

- définir les règles de sécurité pour assurer que les services ou leur exécution ne deviendront pas vulnérables et que l'information traitée sera intègre;
- fixer les exigences de sécurité qu'il faut inclure dans les ententes de niveau de service établies entre le prestataire et le consommateur du service;
- définir le cadre des exigences de sécurité et de protection des renseignements personnels à appliquer aux services.

Fédération de l'information

La fédération de l'information fournit aux utilisateurs une vue unique des données présentes sur plusieurs systèmes d'information, hétérogènes a priori. Elle permet l'intégration de différents systèmes d'information au moyen d'un modèle de référence de l'information gouvernementale en assurant une interopérabilité harmonieuse de ces systèmes.

La fédération de l'information permet de recueillir et de cataloguer l'information sur des contenus structurés et non structurés, localisés dans les différents répertoires gouvernementaux, pour les intégrer dans un modèle commun. Elle permet ainsi :

- ✓ de faciliter la recherche de l'information dans des emplacements multiples grâce à un répertoire commun et à l'agrégation;
- ✓ d'avoir un point d'accès unique à l'information;
- ✓ d'effectuer des mises à jour relatives aux actions complètes du cycle de vie de l'information (ajout, modification, suppression) dans des emplacements multiples;
- ✓ de préserver les investissements initiaux dans la gestion des contenus tout en ayant une vue consolidée de l'information;
- ✓ d'uniformiser la sécurité et l'accès à l'information.

Objectif de sécurité de l'information

- ✓ Prendre en charge les risques en matière de sécurité associés à l'information fédérée afin d'assurer la disponibilité, l'intégrité et la confidentialité de l'information fédérée

  Cet objectif vise à répondre aux préoccupations suivantes :

  - uniformiser la sécurité des accès au système fédéré (systèmes d'information hétérogènes a priori) et définir les mécanismes d'authentification et d'autorisation les plus adéquats;
  - déterminer les exigences de sécurité qui seront prises en charge par les différents partenaires du système fédéré;
  - assurer une interopérabilité sécuritaire entre les systèmes d'information fédérés;
  - reconnaître les risques anticipés de sécurité de l'information en cas de fédération de systèmes de niveaux de criticité différents;
  - analyser l'impact de la complexité des environnements distribués sur la sécurité de l'information fédérée.

Le gouvernement comme une plateforme

Le gouvernement comme une plateforme vise à améliorer la gestion des données fournies par les usagers des services publics en évitant à un usager de transmettre à un organisme public divers renseignements déjà détenus par d'autres organismes publics.

Le gouvernement comme une plateforme simplifie les échanges entre les organismes publics, précisément entre ceux exposant des données par l'intermédiaire d'interfaces (API) et ceux délivrant des services exploitant ces données. Pour orchestrer ces flux d'information, les fournisseurs de données et les fournisseurs de services s'appuieront sur les différentes composantes du gouvernement comme une plateforme, entre autres sur le service d'identification et d'authentification.

Le gouvernement comme une plateforme propose des ressources, notamment un outil pour référencer les API disponibles, préciser la nature des données qu'elles recouvrent et les contrats de service associés. Une forge sera également mise à disposition des développeurs pour favoriser la réutilisation des composants logiciels nécessaires à la construction de services.

Objectif de sécurité de l'information

- ✓ Offrir une plateforme gouvernementale sécuritaire

  Cet objectif vise à répondre aux préoccupations suivantes :

  - assurer que toute initiative associée à la plateforme gouvernementale tiendra compte de la sensibilité de l'information lors des échanges entre les usagers et celle-ci;
  - assurer que le service d'authentification faisant partie de la plateforme gouvernementale permettra à l'usager de s'authentifier adéquatement selon le niveau de confiance requis pour accéder à l'information.

Infonuagique

Une vaste gamme de services infonuagiques[6] matures sont disponibles sur le marché : infrastructures de traitement et de stockage de données, plateformes de développement et nombreuses applications de commodité telles que courriel, téléconférence, téléphone IP, plateformes de collaboration, logiciels de gestion de projets, centre d'assistance, partage de fichiers, etc.

La vision gouvernementale de l'AEG est de tirer profit de l'infonuagique pour accroître l'agilité gouvernementale et pour réaliser des économies en ressources informationnelles tout en assurant la pérennité des actifs informationnels et le respect de la vie privée. Elle encourage le recours à l'infonuagique par les organismes publics qui devront considérer cette possibilité avant d'opter pour le développement de solutions traditionnelles. Cependant, une analyse des risques en matière de sécurité de l'information doit être réalisée avant de prendre la décision de recourir à l'infonuagique et le mode de déploiement approprié devra être déterminé en fonction du degré de sensibilité des données concernées.

Objectif de sécurité de l'information

- ✓ Encadrer les organismes publics dans le choix de solutions infonuagiques sécuritaires

  Pour atteindre cet objectif, plusieurs préoccupations relatives à la sécurité de l'information sont à considérer :

  - La **confidentialité** : l'environnement infonuagique étant caractérisé par une infrastructure partagée, il y a lieu :
    - de s'interroger sur les moyens à mettre en œuvre pour protéger les données sensibles lorsqu'elles sont stockées ou en circulation;

6. Selon l'Office québécois de la langue française (OQLF) : « L'infonuagique est un modèle qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services évolutifs, adaptables dynamiquement et facturés à l'utilisation. »

- de s'assurer que les données conservées en infonuagique seront supprimées adéquatement lorsque les ressources seront attribuées dynamiquement;
- de gérer le chiffrement des renseignements en transit et des clés cryptographiques.

- **La localisation des données :** prévoir les dispositions permettant de réduire l'impact des écarts entre les exigences légales et réglementaires du Québec et celles d'autres États sur les plans de la compétence, de la divulgation des données, des droits de propriété et du maintien de ces droits dans le cas où les actifs d'un client seraient considérés comme ceux du prestataire dans le cas d'une faillite.
- **La gestion du caractère privé des données :** définir les mesures de sécurité de l'information à instaurer pour assurer la protection des renseignements personnels.
- **La disponibilité des services ou de l'information :** définir les critères de choix d'un fournisseur infonuagique à considérer pour éviter de s'exposer à une performance inadéquate, une capacité limitée du réseau, une mauvaise tolérance aux pannes ou un arrêt des services de télécommunication et définir les clauses contractuelles à intégrer dans le contrat de services pour garantir la disponibilité des services du fournisseur infonuagique.
- **Le contrôle des accès :** définir les mesures de sécurité de l'information à appliquer pour assurer un contrôle d'accès adéquat aux données stockées ou traitées en infonuagique.
- **L'environnement multilocataires complexe et les fuites de données :** définir les mesures de sécurité de l'information pour se prémunir contre les risques de fuite de données dans un environnement caractérisé par des ressources partagées entre plusieurs clients et contre les risques de cloisonnement inadéquat de données.
- **La perte de données :** définir les mesures de sécurité de l'information à appliquer pour éviter les conséquences d'une perte de données à la suite de la suppression accidentelle causée par le prestataire d'infonuagique, de désastres naturels ou encore par un ou des intervenants malveillants.
- **La gestion de la chaîne d'approvisionnement :** définir les clauses contractuelles à intégrer dans les contrats avec les prestataires d'infonuagique pour se prémunir contre d'éventuels problèmes concernant l'intégrité de la chaîne d'approvisionnement, qui pourraient rendre les produits infonuagiques vulnérables à la malversation et aux altérations.
- **Les interfaces de programmation d'application (API) non sécurisées :** s'assurer de la prise en considération de la sécurité de l'information dès l'étape de la conception des interfaces utilisées en infonuagique à des fins de surveillance, de prestation ou de gestion afin d'éviter des situations de vulnérabilité exploitables par les cybercriminels.
- **La fiabilité du fournisseur en matière de sécurité de l'information :** s'assurer du niveau de sécurité de l'information que le fournisseur du service infonuagique peut garantir à l'égard de l'information qu'il traite ou à laquelle il a accès.
- **La gestion du changement :** réduire les impacts d'origine humaine, organisationnelle ou technologique sur la sécurité de l'information lors de l'introduction du modèle de livraison de services infonuagiques. À cet effet, plusieurs éléments sont à considérer :
  - la catégorisation des renseignements externalisés;
  - l'irrévocabilité des transactions et le maintien de la valeur probante des documents d'intérêt;
  - la perte de contrôle sur les services infonuagiques ou sur l'information;
  - le partage des responsabilités avec le fournisseur;
  - la responsabilité des fournisseurs en cas d'incidents de sécurité;

- le contrôle des coûts de mise en place de mesures de sécurité de l'information.

- **Le choix de la solution infonuagique :** en ayant recours à un service infonuagique, l'organisme doit accepter une solution dite générique, offerte à de multiples clients, et renoncer à une personnalisation que lui permettrait le développement d'une solution propre à son organisation. Ainsi, il s'avère nécessaire de rapprocher, autant que possible, les besoins en matière de sécurité de l'information d'une offre de services générique.

Sources officielles d'information

La mise en place des sources officielles d'information vise principalement à éviter que les mêmes données soient recueillies plusieurs fois par les organismes publics. Elle permet ainsi la mise en commun de données utiles à un plus grand nombre d'organismes dans des formats pertinents.

Un tel objectif signifie que les systèmes d'information du gouvernement doivent s'ouvrir à leurs partenaires à travers, notamment, des interfaces standardisées. Cela a pour conséquences l'exposition aux risques relatifs à la sécurité de l'information et la nécessité d'instaurer des mesures permettant d'en atténuer l'impact.

Objectif de sécurité de l'information

- ✓ Définir un cadre de gouvernance en sécurité de l'information des sources officielles d'information

  Cet objectif permet d'apporter des éléments de réponse aux préoccupations suivantes :

  - définir les exigences en matière de sécurité de l'information que doit respecter une source officielle d'information, particulièrement en matière de gestion des accès;
  - définir le partage des responsabilités en matière de sécurité de l'information à l'égard des sources officielles d'information;
  - définir les critères de détermination du niveau de confiance d'une source officielle d'information.

Logiciel libre

Le gouvernement du Québec recommande de considérer plus systématiquement le logiciel libre et il en préconise l'utilisation lorsqu'il s'avère le meilleur choix. Il recommande à cet égard la mise en place d'une forge, soit un système de gestion de développement collaboratif de logiciels permettant :

- ✓ le partage de solutions logicielles;
- ✓ de tirer profit de la communauté de personnes qui développent des solutions partageables.

Objectifs de sécurité de l'information

- ✓ Définir les critères d'évaluation de la maturité des logiciels libres en matière de sécurité de l'information

  Cet objectif vise à analyser les risques de sécurité de l'information associés à l'utilisation des logiciels libres et à définir les critères permettant d'en évaluer la maturité en matière de sécurité de l'information. Ces critères permettront également de juger du niveau de maturité en sécurité de l'information des logiciels libres consignés au « catalogue gouvernemental de logiciels libres » et de les intégrer à ce dernier.

- ✓ Encadrer les communautés qui développent des solutions partageables en matière de sécurité de l'information

  Cet objectif vise à mettre à la disposition de ces communautés des pratiques exemplaires d'intégration de la sécurité, des contrôles et de la protection des renseignements personnels dans la conception d'applications basées sur le logiciel libre.

Gouvernement ouvert

Le gouvernement du Québec adopte l'approche du gouvernement ouvert et transparent en vue de rapprocher le citoyen de l'administration publique. Il vise à mettre à la disposition du citoyen des données ouvertes[7] de qualité, dans un format simple à utiliser, afin de faciliter sa participation à l'élaboration de solutions innovantes et d'appuyer le développement économique.

Objectif de sécurité de l'information

- ✓ S'assurer du respect de la protection des renseignements personnels et de la vie privée dans un contexte de libération de données

  Pour ce faire, il importe de répondre aux préoccupations suivantes :

  - encadrer les organismes publics dans le processus d'anonymisation des données ouvertes en vue de garantir le respect de la vie privée et la protection des renseignements personnels;
  - s'assurer que le croisement des données anonymisées ne permet pas l'identification des personnes concernées et la divulgation des renseignements personnels.

Mobilité : BYOD

Le principe du BYOD (*bring your own device*) permet au personnel d'un organisme public d'accéder à sa messagerie professionnelle, à l'intranet ainsi qu'aux applications de l'organisme en employant son propre équipement mobile.

Lors de tout travail à distance, la principale difficulté consiste à faire bénéficier les employés d'accès privilégiés aux applications de la même manière que lorsqu'ils se trouvent dans les locaux de l'organisme. Ces accès doivent être garantis et mis en place grâce à une gestion des droits d'accès adaptée, avec une connexion rapide, pérenne et au débit continu.

Malgré les avantages qu'offre la mobilité, il est important de souligner que des règles et des politiques en matière de sécurité de l'information et de protection des renseignements personnels doivent être adoptées et respectées par tous les utilisateurs du BYOD de l'organisme.

Objectifs de sécurité de l'information

- ✓ Assurer la sécurité de l'information de l'organisme dans un contexte de mobilité des employés

  Pour ce faire, plusieurs éléments sont à considérer, notamment :

  - s'assurer que l'équipement mobile qui se connecte au réseau interne de l'organisme ne présente pas de failles de sécurité;
  - assurer une gestion des droits d'accès adaptée à la mobilité;
  - garder le contrôle sur le parc informatique connecté au réseau de l'organisme;
  - adopter une politique de sécurité de l'information pour encadrer la pratique du BYOD;
  - définir le droit de propriété des fichiers et dossiers produits dans le cadre du BYOD;
  - situer la responsabilité de l'organisme et celle de l'utilisateur du BYOD en cas de vol ou de perte de données professionnelles emmagasinées sur un terminal mobile personnel;

7. Les données ouvertes sont des données brutes non nominatives et libres de droits, produites ou recueillies par un organisme public ou privé et rendues accessibles aux citoyens par Internet [Stratégie gouvernementale en TI, 2015].

- établir des règles de droit permettant à un organisme de supprimer à distance, en totalité ou en partie, les données lui appartenant qui sont stockées dans un appareil mobile;
- mettre en place les mesures permettant d'atténuer tout risque de fuite de données sensibles accessibles ou emmagasinées sur un terminal mobile, notamment les droits d'administration des équipements mobiles, le chiffrement du contenu de l'équipement mobile, la géolocalisation des équipements mobiles, l'identification des personnes accédant à l'équipement mobile, les règles de gestion de l'incident en cas de vol, perte ou corruption des données de l'organisme contenues sur le terminal mobile.

✓ Sensibiliser les utilisateurs de terminaux mobiles à la protection de l'information à l'égard de toute tentative d'indiscrétion

Il est important que les utilisateurs du BYOD prennent conscience de la vulnérabilité à laquelle ils s'exposent lors de l'utilisation de leurs appareils mobiles dans les lieux publics à des fins professionnelles, surtout en cas d'accès à des données sensibles de l'organisme. À titre d'exemple, la lecture par-dessus l'épaule peut révéler les mots de passe, surtout que le dernier caractère tapé est en général affiché par défaut à l'écran.

Web participatif et collaboratif (collaboration sociale)

L'utilisation des réseaux sociaux est d'actualité et donne lieu au partage, à la diffusion ou à la cocréation de documents ou d'applications. À cet effet, le réseau social d'entreprise permet l'accès aux applications, au courriel et à la messagerie instantanée de l'entreprise. Cette tendance met de la pression sur les organismes pour intégrer les outils de collaboration dans le milieu de travail.

Objectif de sécurité de l'information

✓ Déterminer les règles de gouvernance de la sécurité de l'information en matière de collaboration sociale

À cet égard, il importe de répondre :

- aux exigences de propriété, de sécurité et de fiabilité de l'information publiée;
- aux besoins associés au respect de la vie privée et à la protection des renseignements personnels;
- aux besoins en matière d'identification et d'authentification.

Mise en place des infrastructures communes

Dans une perspective d'économie d'échelle, l'AEG préconise :

✓ de regrouper et de centraliser la gestion des centres de traitement informatique existants dans les centres plus performants et moins coûteux;

✓ de consolider et rationaliser le stockage des données afin d'optimiser les centres de stockage de données par l'utilisation généralisée des techniques de virtualisation.

Objectif de sécurité de l'information

✓ Définir un cadre de gestion des risques en matière de sécurité de l'information associés aux infrastructures communes

La mise en place des infrastructures communes entraîne des répercussions sur le périmètre de sécurité traditionnel des organismes. En effet, la suppression des barrières de sécurité auparavant strictement définies et séparées au sein d'une organisation présente des défis relatifs à la gestion des risques en matière de sécurité de l'information, notamment :

- l'augmentation de la surface d'attaque des réseaux et des systèmes avec pour conséquence le risque de perturbation ou d'interruption des services;
- le risque de dégradation de la qualité du service découlant du partage d'infrastructures;
- le risque de confusion en ce qui concerne l'attribution des responsabilités en sécurité de l'information et la reddition de comptes;
- la complexification de la gestion des incidents et des interventions dans des environnements interconnectés;
- la prise en charge des préoccupations relatives à la sécurité de l'information associées aux environnements virtualisés.

Interopérabilité

L'interopérabilité[8] représente un aspect incontournable de l'intégration technologique des services en ligne, lesquels demandent d'ouvrir et de faire coopérer les systèmes d'information des différents organismes publics. Elle favorise les interactions entre les organismes et permet une meilleure exploitation des possibilités de partage et de réutilisation des ressources informationnelles et, de ce fait, une meilleure prestation de services intégrée.

Ainsi, un service ne peut être mis en commun si ses composants applicatifs et d'infrastructures ne sont pas compatibles avec l'infrastructure technologique des organismes publics qui veulent l'utiliser. Pour ce faire, la détermination des normes et des standards relatifs à chaque service partagé s'avère nécessaire pour assurer son interopérabilité avec les systèmes d'information des organismes publics utilisateurs. De même, les services et applications ayant une portée gouvernementale potentielle doivent être conçus et développés de façon à « interopérer » avec tous les systèmes d'information des organismes publics.

Objectif de sécurité de l'information

- ✓ Déterminer les exigences visant à assurer une interopérabilité sécuritaire entre les services gouvernementaux

  Cela consiste à préciser les exigences de sécurité que les normes et standards d'interopérabilité doivent satisfaire pour garantir la confidentialité et l'intégrité de l'information traitée par les services d'échanges sur le Web et pour assurer l'authentification des entités ainsi que la non-répudiation des renseignements ou des actions échangés.

4.2.2 Lignes directrices du segment Sécurité

Les lignes directrices en sécurité de l'information associées aux volets Affaires, Information, Applications et Infrastructures découlent de l'analyse des préoccupations relatives à la sécurité de l'information engendrées par les orientations de l'architecture cible de l'AEG. Elles véhiculent les attentes gouvernementales en matière de sécurité de l'information en vue de prendre en charge ces préoccupations.

Plusieurs travaux concernant la sécurité de l'information sont réalisés en soutien aux volets Affaires, Information, Applications et Infrastructures. Leur liste est présentée en annexe.

8. L'interopérabilité est définie comme « la possibilité pour des systèmes informatiques hétérogènes d'échanger des données et des services informatiques » [Cadre commun d'interopérabilité du gouvernement du Québec].

   L'Office québécois de la langue française définit l'interopérabilité comme « la faculté qu'ont des systèmes de fonctionner conjointement et de donner accès à leurs ressources de façon réciproque ».

Volet Affaires

- ✓ Les solutions de sécurité de l'information soutiennent la mise en œuvre des processus d'affaires de l'organisme public sans en entraver l'évolution.
- ✓ La protection adéquate de l'information exige la compréhension de l'environnement, des risques courus, de la criticité des systèmes et des processus et de l'information.
- ✓ La consolidation de la confiance des citoyens et des entreprises à l'égard de l'État est assurée par la robustesse des dispositifs mis en place pour la sécurisation des systèmes.
- ✓ Les accès des citoyens et des entreprises aux services gouvernementaux sont sécurisés quel que soit le mode de prestation offert.
- ✓ L'accès à l'offre gouvernementale de services en ligne est assuré par une identification et une authentification de l'usager.
- ✓ L'architecture de sécurité de l'information favorise l'utilisation de nouveaux modes d'acquisition de services et l'interopérabilité de ces services ainsi que les échanges sécuritaires de l'information.
- ✓ Les services du gouvernement doivent être conçus de façon à définir clairement et sans chevauchement les responsabilités et le lien de confiance entre les parties prenantes.

Volet Information

- ✓ Les règles de sécurité de l'information associées aux sources officielles d'information gouvernementale sont clairement définies et une autorité désignée devra rendre compte de leur application.
- ✓ Les risques de sécurité de l'information associés au système d'information fédéré sont analysés et les exigences de prise en charge par les différents partenaires sont précisées.
- ✓ L'usager s'authentifie avec le niveau d'exigence de sécurité souhaité selon la sensibilité de l'information à laquelle il a accès.
- ✓ Le respect de la protection des renseignements personnels et de la vie privée doit être assuré lors de la libération des données gouvernementales afin d'éviter l'identification directe ou indirecte d'un individu par le croisement des données ouvertes.
- ✓ L'information recueillie auprès de l'usager est sécurisée sans égard au mode de prestation de service utilisé (service au comptoir, en ligne ou par téléphone).
- ✓ La détermination de la valeur des actifs informationnels est essentielle à la mise au point de solutions de sécurité robustes.
- ✓ Tout échange d'information gouvernementale (entre une clientèle et le gouvernement ou entre les organismes publics) est sécurisé selon le niveau de sensibilité de l'information échangée.

Volet Applications

- ✓ Les solutions de sécurité doivent être adaptées à l'approche de développement, notamment l'approche orientée services.
- ✓ Les risques de sécurité de l'information associés à un projet de développement doivent être pris en considération dès l'étape de l'analyse et tout au long de sa réalisation.
- ✓ Les services applicatifs communs sont facilement repérables et interopérables. À cet effet, les règles, les normes et standards d'interopérabilité qu'ils doivent respecter sont clairement définis en vue de leur réutilisation et de leur publication à l'échelle gouvernementale.
- ✓ La disponibilité, confidentialité et l'intégrité de l'information traitée ou échangée par les applications sont prises en considération et assurées dès l'étape de la conception de la solution.

- ✓ Le niveau de maturité en matière de sécurité de l'information des logiciels libres consignés au « catalogue gouvernemental des logiciels libres » doit être évalué et intégré à ce catalogue.
- ✓ Les risques de sécurité des outils de collaboration et des solutions d'infonuagique sont évalués et pris en considération lors du choix des solutions.

Volet Infrastructures

- ✓ Les règles de sécurité de l'information des infrastructures communes sont clairement définies et diffusées à l'échelle gouvernementale.
- ✓ Des éléments d'encadrement de la prise en charge des risques de sécurité de l'information propres à l'utilisation des services infonuagiques doivent être élaborés et portés à la connaissance des organismes publics.
- ✓ Les règles de sécurité à respecter par le modèle[9] d'architecture « Infrastructure orientée services » sont clairement définies.
- ✓ Les messages échangés lors des interactions entre les composantes d'infrastructures doivent être sécurisés et leur origine retraçable et non répudiable.
- ✓ Les normes et standards de sécurité de l'information adéquats et interopérables sont utilisés afin d'accroître l'efficacité et la cohérence de la sécurité de l'information gouvernementale et la protection des renseignements personnels.

5. Apport de l'ASIG à l'architecture de sécurité de l'information sectorielle

Bénéfices découlant de l'élaboration d'une architecture de sécurité de l'information sectorielle (à portée ministérielle ou organisationnelle)

Plusieurs éléments plaident en faveur de la mise en place d'une architecture de sécurité de l'information sectorielle. Citons à cet égard :

- ✓ Les solutions de sécurité de l'information sont souvent conçues, acquises ou installées sur une base tactique qui se traduit généralement par la mise en place d'une solution répondant à un besoin particulier de sécurité de l'information. Une architecture de sécurité de l'information sectorielle offre la possibilité d'obtenir une vue d'ensemble permettant d'examiner la dimension stratégique de l'ensemble des solutions et d'en assurer la compatibilité et l'interopérabilité. Elle permet aussi d'envisager une analyse des coûts à long terme et de déterminer une stratégie afin de soutenir les objectifs d'affaires de l'organisme.
- ✓ L'implémentation de bons processus et de solutions de choix en sécurité de l'information est assurée lorsqu'ils sont alignés sur les stratégies d'affaires de l'organisme.

9. Le modèle d'architecture d'IOS décrit l'infrastructure technologique en termes de services à différents niveaux (découpage, attribution, utilisation et gestion). L'objectif de l'architecture IOS est de fournir un regroupement de ressources virtualisées et partageables découpé en services d'infrastructure pour faciliter leur réutilisation. Les services d'infrastructure peuvent être découpés, par exemple, en unités logiques ou fonctionnelles telles que : serveur, réseau, stockage, logiciel d'infrastructure, etc. Ces services d'infrastructure sont déployés et gérés de façon hautement standardisée et automatisée; de plus, un soutien de base est offert à l'architecture orientée services, et plus précisément aux services applicatifs.

- ✓ L'utilisation de l'évaluation des risques dans le processus de planification de l'évolution de l'architecture de sécurité de l'information permet d'offrir une architecture souple, alignée en continu sur les besoins d'affaires de l'organisme en plus d'éviter l'obsolescence.
- ✓ L'architecture de sécurité procure à l'organisme un plan directeur de ce qui doit être fait en matière de sécurité de l'information.

Par ailleurs, l'architecture de sécurité de l'information n'est plus associée exclusivement au volet technologique (solutions de sécurité implémentées), mais elle est de plus en plus utilisée pour construire une feuille de route pour la mise en place d'une sécurité de l'information efficace alignée sur les objectifs d'affaires fixés par l'architecture d'entreprise de l'organisme. Ainsi, l'architecture de sécurité offre un cadre dans lequel les besoins d'affaires en matière de sécurité de l'information et les risques sont analysés. Par la suite, un ensemble intégré de meilleures solutions de sécurité de l'information est mis en place.

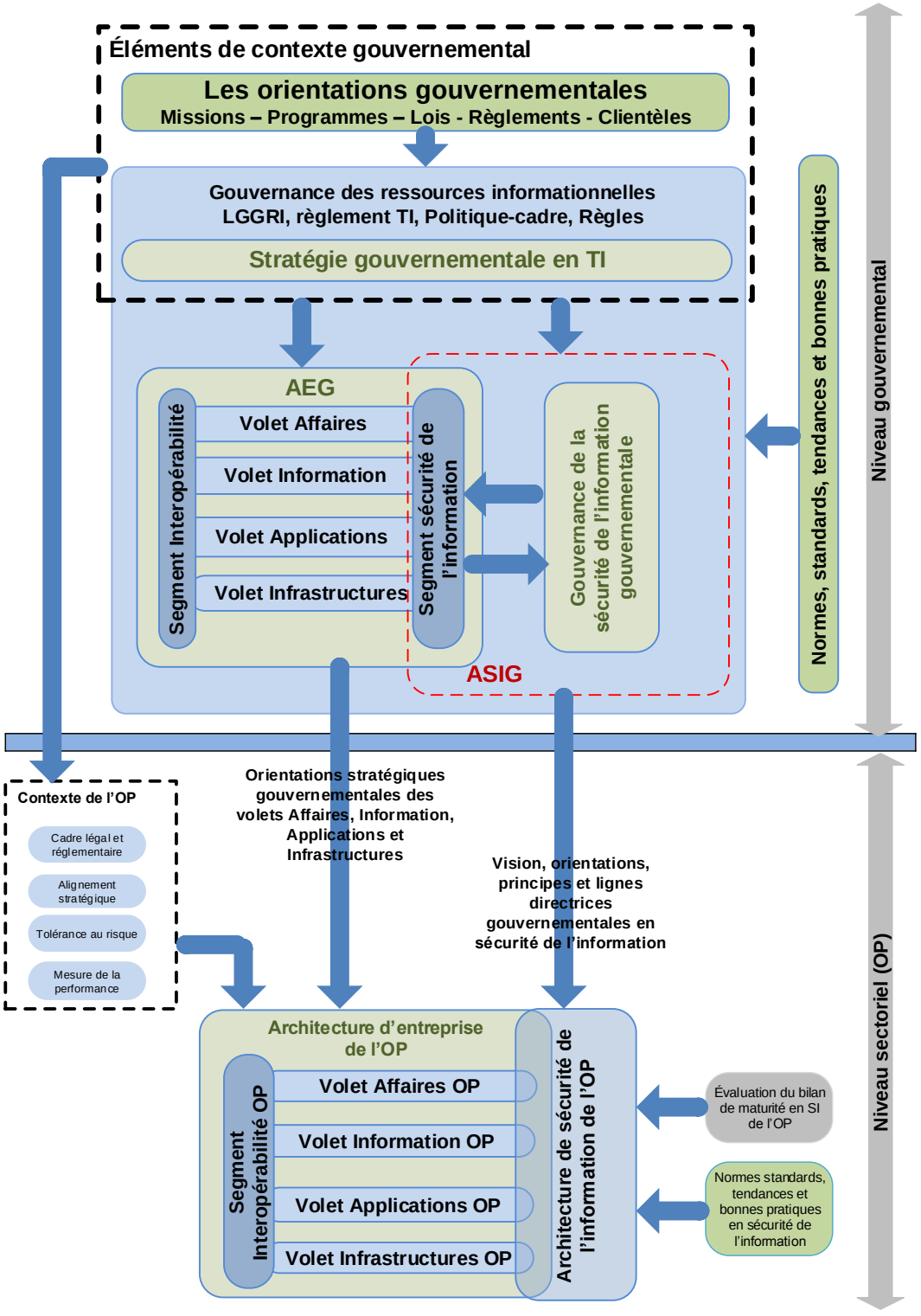
Un processus d'architecture efficace doit reposer sur des principes cohérents, des mécanismes et des lignes directrices permettant d'aboutir à des solutions de sécurité efficaces, coordonnées et appropriées aux besoins d'affaires de l'organisme et tenant compte risques courus en matière de sécurité. Cette approche itérative où chaque version couvre un niveau d'abstraction de plus en plus détaillé (affaires, conceptuel, logique puis implémentation) permet d'établir un lien entre les solutions de sécurité implémentées, les orientations et les besoins d'affaires initiaux.

Définition de l'architecture de sécurité de l'information sectorielle

L'architecture de sécurité de l'information est un outil stratégique qui définit la vision et les orientations en sécurité de l'information de l'organisme public. Elle est alignée sur les orientations gouvernementales et tient compte des objectifs d'affaires de l'organisation et des risques de sécurité associés. Elle permet de circonscrire les préoccupations de l'organisation en matière de disponibilité, d'intégrité et de confidentialité de l'information et, ainsi, de contribuer à l'élaboration et à la mise en œuvre d'un programme (plan directeur) de sécurité de l'information cohérent et intégré.

Note : L'architecture de sécurité de l'information sectorielle est élaborée selon un processus itératif qui tient compte de l'évolution de l'architecture d'entreprise. Elle est idéalement articulée autour des volets Affaires, Information, Applications et Infrastructures de l'architecture d'entreprise, lesquels intègrent, mais sans s'y limiter, les préoccupations de partage sécuritaire de l'information, de protection de l'accès à l'information, de sécurisation des réseaux et des infrastructures, de sécurisation des applications et des systèmes d'information, de continuité des affaires et de journalisation des opérations.

Figure 2 : Lien entre l'ASIG et l'ASIS



Conformément à la figure 2, l'architecture de sécurité de l'information sectorielle tient compte de l'architecture de sécurité de l'information gouvernementale et s'adapte à sa propre architecture d'entreprise.

Apport de l'ASIG

L'ASIG sert de référence aux organismes publics pour la conception et la mise en œuvre d'une architecture de sécurité de l'information sectorielle, alignée sur la vision gouvernementale et qui serait à la base de la mise en œuvre d'un programme de gestion de la sécurité de l'information suffisamment mature pour atteindre les objectifs suivants :

- ✓ **atténuation des menaces :** reconnaître et résoudre les menaces critiques rencontrées par l'organisme en matière de sécurité de l'information;
- ✓ **confiance accrue :** donner confiance aux gestionnaires et autres parties prenantes à propos du respect des exigences de sécurité;
- ✓ **validation des actifs :** définir et valider les technologies de l'information versus les investissements en sécurité de l'information;
- ✓ **amélioration de la conformité en matière de sécurité :** respect des lois et règlements et alignement avec les bonnes pratiques en sécurité de l'information ainsi que les orientations gouvernementales en la matière;
- ✓ **durabilité :** faire en sorte que le programme de gestion de la sécurité soit opérationnel et demeure viable à long terme en mettant l'accent sur l'amélioration constante et l'alignement continu avec les objectifs d'affaires de l'organisme;
- ✓ **garantie de traçabilité :** la surveillance continue des indicateurs de performance de la mise en œuvre de la feuille de route élaborée en architecture de sécurité fournit la traçabilité des objectifs d'affaires de l'organisme jusqu'aux solutions technologiques de sécurité.

ANNEXE Documents élaborés

- ✓ Guide d'élaboration d'une politique de sécurité de l'information
- ✓ Guide d'élaboration d'un cadre de gestion en sécurité de l'information
- ✓ Guide établissant les critères de désignation des principaux intervenants en sécurité de l'information (ROSI, COSI et ALT)
- ✓ Guide d'élaboration d'un bilan ministériel de sécurité de l'information
- ✓ État de situation bisannuel de la sécurité de l'information gouvernementale
- ✓ Guide de mise en œuvre du cadre de gestion des risques de sécurité de l'information à portée gouvernementale
- ✓ Rapport sur les risques de sécurité de l'information à portée gouvernementale
- ✓ Guide d'élaboration d'un tableau de bord en sécurité de l'information
- ✓ Tableau de bord en sécurité de l'information
- ✓ Guide de mise en place d'un processus de gestion des incidents de sécurité de l'information
- ✓ Guide de mise en place d'un processus de gestion des risques de sécurité de l'information
- ✓ Guide de mise en place d'un processus de gestion des accès logiques
- ✓ Guide de rédaction de clauses contractuelles en matière de sécurité de l'information
- ✓ Orientations et stratégie d'authentification des citoyens et entreprises dans le cadre du gouvernement électronique
- ✓ Guide de continuité des services
- ✓ Guide de catégorisation de l'information
- ✓ Guide de destruction sécuritaire de l'information
- ✓ Guide de sensibilisation à la sécurité de l'information
- ✓ Guide et outil pour la prise en charge des exigences de SCPRP dans le cycle de développement ou d'acquisition d'un système d'information
- ✓ Guide de mise en œuvre des tests d'intrusion et de vulnérabilité
- ✓ Guide d'audit de la sécurité de l'information
- ✓ Guide d'utilisation des assistants numériques personnels
- ✓ Guide de l'infonuagique - Volume 3 : Considérations de contrôle et de sécurité

Ces documents sont disponibles sur les sites suivants :

- ✓ Communauté des dirigeants de l'information et leur entourage https://di.collaboration.gouv.qc/
- ✓ Communauté de sécurité de l'information https://comsi.collaboration.gouv.qc/groupes/bonnes-pratiques/bibliotheque/
- ✓ Réseau d'experts et de vigie en sécurité de l'information http://www.securite.gouv.qc.ca

Secrétariat
du Conseil du trésor
Québec