Politique gouvernementale de cybersécurité

Demi-journée Cybersécurité

Les nouveautés de 2020 en Cybersécurité

ISACA – Section de Québec

27 octobre 2020

Christiane Langlois
Directrice générale de la sécurité de l'information gouvernementale
Secrétariat du Conseil du trésor

Votre gouvernement

Québec

Mise en contexte

- Stratégie de transformation numérique gouvernementale
- Augmentation de la prestation électronique de services
- Plusieurs incidents de confidentialité impliquant des renseignements personnels

Votre gouvernement

Québec

Mise en contexte (suite)

Face aux enjeux de cybersécurité internes et externes, des moyens s'imposent pour :

- mobiliser l'ensemble des acteurs de l'écosystème de cybersécurité
- innover dans la prise en charge des risques de cybersécurité, et ce, dans un processus d'amélioration continue
- intervenir de façon proactive en anticipant les menaces et en adaptant constamment les moyens de s'en protéger
- favoriser et encourager les actions de sensibilisation qui visent à promouvoir l'adoption de comportements sécuritaires auprès de la population et du personnel de l'État

Portée

- S’applique à l’ensemble des organismes publics assujettis à la *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)
- Concerne aussi les relations de ces organismes avec les usagers des services publics et avec leurs partenaires
- Le Secrétariat du Conseil du trésor est responsable de sa mise en œuvre à l’échelle gouvernementale
- La Politique est appuyée par des mesures clés

Objectif

La Politique gouvernementale de cybersécurité vise à instituer une Administration gouvernementale **résiliente** et cyberprotégée qui offre des services numériques centrés sur la personne

Résilience : capacité des systèmes à résister ou à se relever en cas d'incident

Principes fondamentaux

- PRINCIPE 1 - Assurer l'application de mesures de protection proportionnelles à la valeur de l'information et aux risques encourus
- PRINCIPE 2 - Favoriser et encourager l'adoption de comportements cybersécuritaires
- PRINCIPE 3 - Miser sur le développement des compétences, l'attraction et la rétention des talents
- PRINCIPE 4 - Encourager le partage et la mise en commun
- PRINCIPE 5 - Intégrer la protection de l'information en amont

Axe 1 - La cybersécurité, une priorité gouvernementale

Votre gouvernement

Québec

Objectif 1 - Gouverner la cybersécurité par une vision globale et concertée

Adopter une gouvernance qui s’appuie sur une vision globale et concertée simplifie la gestion des risques encourus et assure une meilleure protection de l’information.

Quelques implications :

- Adapter le cadre législatif et réglementaire
- Réviser le cadre de gestion de la sécurité de l’information
- Soutenir et accompagner les organisations publiques

Objectif 2 - Placer le personnel au cœur de la cybersécurité

L'Administration gouvernementale entend faire du personnel de l'État un acteur averti quant aux comportements et aux pratiques exemplaires à adopter devant les cybermenaces.

Quelques implications :

- L'ensemble du personnel de l'État comme maillon fort de la cybersécurité
- Des actions de prévention et de promotion de la cyberhygiène dans les milieux de travail

Votre gouvernement

Québec

Axe 2 - Des services publics sécuritaires

Votre gouvernement

Québec

Objectif 3 - Assurer la protection et la résilience des services publics et des échanges électroniques gouvernementaux

Devant les enjeux de cybersécurité, des mesures à l'égard des risques et des menaces internes et externes s'imposent.

Quelques implications :

- Un processus rigoureux de gestion des cyberrisques
- La mise en place de mesures d'atténuation des risques
- Des réseaux de télécommunication assurant une protection adéquate
- Une gestion de l'identité et des accès prenant appui sur une identité numérique
- La protection de l'information et la résilience des systèmes dès leur conception

Objectif 4 - Être proactif à l'égard des menaces émergentes

Le gouvernement entend augmenter les capacités institutionnelles d'analyse des risques émergents et de prospective et mettre en place les mesures préventives appropriées de protection et de renforcement de la résilience de ses systèmes.

Quelques implications :

- Établir des liens avec certains partenaires de confiance afin de constituer un réseau d'alerte
- Fédérer des initiatives de recherche et de veille en matière de cybersécurité

Objectif 5 - Miser sur les forces d'un réseau gouvernemental de cyberdéfense

Le renforcement des dispositifs de prévention et de réaction à l'égard des cybermenaces, requiert la mise en place d'un réseau gouvernemental de cyberdéfense, sous le leadership d'une structure gouvernementale de commandement.

Quelques implications :

- Coordonner les efforts en cybersécurité
- Jouer un rôle collaboratif dans l'écosystème de cybersécurité
- Mettre en place un processus de communication aux autorités concernées

Votre gouvernement

Québec

Objectif 6 - Tirer profit d'une expertise de pointe en cybersécurité

Pour réussir la transformation numérique gouvernementale, il est nécessaire d'avoir une main-d'œuvre hautement qualifiée en sécurité de l'information.

Quelques implications :

- Cibler les champs de compétences requis en cybersécurité
- Diversifier les profils et domaines de compétences du personnel en cybersécurité
- Offrir des programmes de formation
- Déterminer le parcours de personnes susceptibles de renforcer le bassin gouvernemental de ressources en cybersécurité
- Évaluer en continu les moyens de formation et les compétences acquises

Axe 3 - Des citoyennes et citoyens confiants et avertis

Votre gouvernement

Québec

Objectif 7 - Préserver la confiance des citoyennes et citoyens à l'égard de la sécurité de leurs données

Le gouvernement entend préserver cette confiance par son engagement de transparence en faveur d'une utilisation éthique et par l'intégration de pratiques exemplaires pour en assurer la protection.

Quelques implications :

- Fournir à toute personne une identité numérique
- Faciliter l'accès par toute personne aux données qui la concernent
- Permettre à toute personne de mettre à jour les données que le gouvernement détient à son égard

Objectif 8 - Faire des citoyennes et citoyens des utilisateurs numériques avertis

Le gouvernement entend mener des actions de sensibilisation à l'égard du public afin que celui-ci acquière des habitudes et des comportements sécuritaires qui contribuent à accroître sa confiance dans ses relations numériques avec l'État.

Quelques implications :

- Rendre des contenus informatifs accessibles au public
- Stimuler l'acquisition des compétences du public
- Assurer que les interactions numériques entre l'Administration gouvernementale et le public soient connues, standardisées et sécuritaires

Votre gouvernement

Québec

Axe 4 - Des partenariats stratégiques et durables

Objectif 9 - Tirer avantage des forces de l'écosystème

Le gouvernement entend tirer avantage des forces de l'écosystème en tissant des alliances stratégiques afin de faire du Québec un espace de conception de solutions innovantes en cybersécurité.

Quelques implications :

- Assurer une synergie pour l'atteinte de buts communs avec les partenaires
- Rallier les organisations dans la détermination de pistes de solution
- Maximiser les retombées

Votre gouvernement

Québec

Questions

Votre gouvernement

Québec