Processus de sécurisation de l'Information

Contexte :

- Le décret 596-2020 du 10 juin 2020 autorise Infrastructures technologiques Québec (ITQ) à débuter la consolidation des centres de traitement informatique en prenant appui *en priorité* sur les offres *infonuagiques externes* (service infonuagique offert par les fournisseurs), ou, si cela n'est pas souhaitable de l'avis de ITQ, à la suite des *revues diligentes*, (examens approfondis du choix de l'OP sous les aspects technologiques et de sécurité) sur le *nuage gouvernemental* (service infonuagique offert par le gouvernement du Québec dans les CTI de l'ITQ) qu'il aura mis en place.
- La non exposition du portail de gestion du nuage gouvernemental à Internet offre une meilleure protection de l'information gouvernementale à l'égard des cyberattaques.
- Pour le nuage externe : les fournisseurs sont qualifiés par le courtier d'infonuagique (ITQ) suivant leur capacité à offrir les niveaux de sécurité exigés.
- À l'opposé du nuage externe, la mutualisation des infrastructures du nuage gouvernemental est réservée à notre communauté.

1 Identifier les actifs et évaluer la sensibilité de l'information gouvernementale

La sensibilité de l'information est évaluée par l'organisme public selon le préjudice qu'il encourt en termes de ***disponibilité***, d'***intégrité*** et de ***confidentialité*** **(DIC)**.

Information non sensible

La compromission engendre des préjudices faibles ou très faibles: information destinée au public dont la compromission de la disponibilité ou de l'intégrité peut engendrer la perte de confiance du public, des pertes financières négligeable, un inconfort physique ou un stress pour le citoyen, etc.

Exemples:

- Résultat d'appel d'offres
- Agenda du personnel
- Affichage de concours de la fonction publique

Information sensible

La compromission engendre des préjudices modérés c'est à dire affecte la santé physique ou mentale ou financière du citoyen, le rendement de l'économie, la compétitivité des entreprises ou engendre des pertes financières importantes, des émeutes, etc.

Exemples:

- Information du citoyen(NAS, adresse, nom, prénom, date de naissance, etc.)
- Déclaration d'impôt
- Information sur la COVID

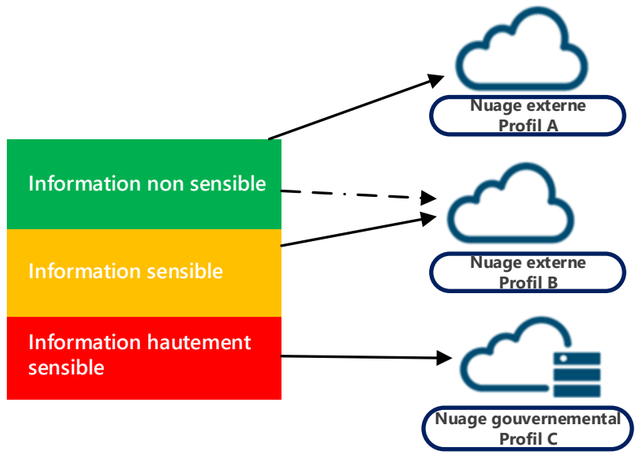
Information hautement sensible

La compromission engendre de lourdes pertes en vie humaine, de lourdes pertes financières, une crise économique, des émeutes généralisées, etc.

Exemples :

- Liste des juges et leur adresse,
- Fichier des délateurs,
- Adresse de refuge des femmes battues,
- Centre antipoison

2 Choisir le modèle infonuagique approprié



Les modèles d'infonuagique (nuage externe ou gouvernemental) et les profils de *mesures minimales* de sécurité de l'information correspondants (profil A, B ou C) sont préalablement déterminés par l'ITQ. L'organisme public choisit le modèle d'infonuagique ainsi que le profil des mesures minimales correspondant selon le niveau de sensibilité de l'information. Les mesures minimales vont croissant du profil A au profil C et sont proportionnelles aux risques encourus.

3 Assurer une revue diligente conjointe (ITQ/OP)

Une analyse est conjointement réalisée par l'organisme public détenteur de renseignements personnels et l'ITQ quant au choix du mode de traitement et de stockage et des mesures de sécurité applicables.

4 Déterminer les responsabilités

Les responsabilités des parties prenantes (OP, fournisseur, ITQ) sont clairement déterminées par l'organisme public, en fonction du modèle d'infonuagique retenu et du profil correspondant.

5 Gérer les risques de sécurité de l'information

Le passage en mode exploitation de la solution infonuagique retenue par l'OP ne peut se faire sans que ce dernier ait l'assurance que les risques afférents sont analysés, qu'ils sont acceptés, aussi bien par lui-même qu'au plan gouvernemental, et qu'un processus de surveillance continue de leur évolution est mis en place.

Stratégie gouvernementale de déploiement dans l'infonuagique

Exemple: Système de dotation en personnel

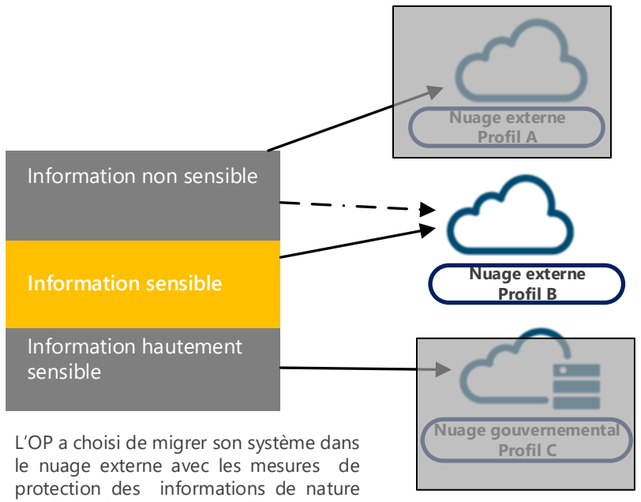
Contexte : Le système d'information permet de gérer les concours de la fonction publique et d'effectuer les dotations en personnel. Il traite et stocke notamment les informations du citoyen (NAS, nom et prénom, adresse, diplômes, etc.).

1 Identifier les actifs et évaluer la sensibilité de l'information gouvernementale

La compromission de la confidentialité ou de l'intégrité peut engendrer des préjudices modérés. L'information est classée **« sensible »**.

Information non sensible	Information sensible	Information hautement sensible
La compromission engendre des préjudices faibles ou très faibles: information destinée au public dont la compromission de la disponibilité ou de l'intégrité peut engendrer la perte de confiance du public, des pertes financières négligeable, un inconfort physique ou un stress pour le citoyen, etc.	La compromission engendre des préjudices modérés c'est à dire affecte la santé physique ou mentale ou financière du citoyen, le rendement de l'économie, la compétitivité des entreprises ou engendre des pertes financières importantes, des émeutes, etc.	La compromission engendre de lourdes pertes en vie humaine, de lourdes pertes financières, une crise économique, des émeutes généralisées, etc.

2 Choisir le modèle infonuagique approprié



L'OP a choisi de migrer son système dans le nuage externe avec les mesures de protection des informations de nature **sensible**, répondant au **Profil B**.

3 Assurer une revue diligente conjointe (ITQ/OP)

Une revue diligente du choix de l'OP est conjointement réalisée par ce dernier et l'ITQ. Des ajustements sont encore possibles à cette étape.

4 Déterminer les responsabilités

L'OP a déterminé les responsabilités suivantes :

- Le fournisseur offre la capacité de chiffrer les données stockées
- L'organisme public chiffre les données stockées avec ses propres clés de chiffrement

5 Gérer les risques de sécurité de l'information

L'OP procède à une analyse des risques pour :

- Rechercher de nouvelles failles de sécurité et les corriger
- Identifier de nouvelles menaces
- Déployer les mesures supplémentaires de protection
- Mettre en place un processus de surveillance de l'évolution des risques de sécurité
- Passer en mode exploitation après avoir accepté les risques résiduels