LA CATÉGORISATION DES INFORMATIONS INSTITUTIONNELLES DE L'UQAM

Un projet de collaboration Archives - informatique

Cynthia Couture, Service des archives et de gestion des documents

Stéphane Talbot, Bureau de la sécurité et de la gouvernance des systèmes d'information

UQÀM | Université du Québec à Montréal

Plan de la présentation

- Le projet
- Le modèle de catégorisation
- Le registre de catégorisation des informations
- Validation et officialisation du registre : Les enjeux et notre approche
- La catégorisation et la sécurité informatique
- Prochaines étapes

Le projet

- Collaboration entre l’équipe informatique et le Service des archives
- Positionnement du Service des archives dans la gestion de l’information
- Pertinence du plan de classification institutionnel
- Grandes étapes du projet
  - Révision de la politique sur la gestion de l’information institutionnelle
  - Élaboration du modèle de catégorisation
  - Élaboration du registre
  - Validation et officialisation du registre

Le modèle de catégorisation

- Niveau de criticité des informations selon 3 aspects : confidentialité, intégrité et disponibilité
- Évaluation de la confidentialité :
  - Informations personnelles
  - Informations à usage restreint
  - Informations à usage interne
  - Informations publiques
- Évaluation de l'intégrité et de la disponibilité selon 4 niveaux:
  - Impacts sur la santé, la sécurité des personnes ou sur la capacité de l'UQAM à réaliser sa mission
  - Impacts académiques et institutionnels : impacts majeurs sur le plan académique, éthique, financier, juridique ou réputationnel
  - Impacts sur la performance d'un nombre importants d'employés ou d'unités
  - Impacts mineurs pour l'institution

Le modèle de catégorisation : Les principes

Point le plus sensible	**Lors de la catégorisation d'un regroupement d'informations, il convient de toujours utiliser le point d'information le plus sensible à l'intérieur du regroupement.**
Pire des scénarios	Lors de la catégorisation d'un regroupement d'informations, l'approche « pire des scénarios » doit être utilisée. Cette méthode consiste à faire abstraction de toutes méthodes de protection déjà existantes couvrant cette information. Prenons le cas d'informations étant déjà couvertes par une procédure de copie de sécurité. Pour réaliser l'évaluation de cette information en termes de disponibilité, il faut faire abstraction de cette mesure de protection en classifiant l'information.
Indépendance des attributs	Chacun des trois attributs de l'information (confidentialité, intégrité, disponibilité) doit être évalué individuellement. Le résultat d'une évaluation n'a aucune incidence sur les deux autres et ne doit en aucun cas être pris en compte. Certaines informations peuvent être de nature peu confidentielle, mais très critiques en termes de disponibilité.
Du plus haut niveau au plus bas	La catégorisation d'un groupement d'information doit se faire en analysant la définition du premier niveau de la dimension. Si celle-ci s'applique, il s'agit de la catégorisation à assigner. Sinon, il faut passer à la seconde et ainsi de suite.

Le registre de catégorisation

- Identifie de façon formelle les informations institutionnelles
- Détermine qui sont les responsables institutionnels des informations
- Disponible pour tous les employés via un wiki

Cote	Processus	Description	Fiduciaire	Confidentialité	Disponibilité	Intégrité
140	Organigramme et structure organisationnelle	Informations utilisées pour élaborer, documenter et assurer l'évolution des structures organisationnelles et administratives de l'UQAM et de ses unités	Unité académique ou administrative responsable	Usage interne	Impacts mineurs sur l'institution	Impacts mineurs sur l'institution
218	Dossiers du personnel	Informations nominatives utilisées pour assurer la gestion et le suivi de la carrière d'un employé à l'UQAM, depuis son embauche jusqu'à son départ.	Ressources humaines	Renseignements personnels	Impacts sur la santé/sécurité et la mission	Impacts sur la santé/sécurité et la mission
716	Dossiers étudiants	Informations nominatives relatives à chaque étudiant et qui constituent son dossier personnel permettant de retracer son cheminement depuis son admission jusqu'à son départ de l'établissement.	Registraire	Renseignements personnels	Impacts académiques et institutionnels	Impacts académiques et institutionnels

Validation et officialisation du registre : Les enjeux

- Réaliser l’opération dans un délai raisonnable
- Évaluer les informations de façon objective
- Optimiser les ressources impliquées
- Catégorisation des informations académiques et de recherche

Validation et officialisation du registre : Notre approche

- Élaboration d’un projet de registre par notre équipe
- Projet pilote de validation de l’approche avec 4 unités
- Envoi des propositions à chacun des responsables pour validation

La catégorisation et la sécurité informatique

- La sécurité informatique n'est pas uniquement la « sécurité des ordinateurs »
- La sécurité de l'information et la catégorisation s'appuient sur la même triade: confidentialité, intégrité et disponibilité.
- Les mesures de sécurité disponibles sont diverses et différenciées en fonction des aspects et du niveau de criticité.
  - Confidentialité : Chiffrement des données
  - Intégrité : Journalisation
  - Disponibilité : Copies de sauvegarde
- La catégorisation nous aide à prioriser nos actions et à développer nos approches de sécurité.

Application au thème de l’infonuagique

- La catégorisation a été utile dans notre approche envers l’infonuagique.
- Afin d’adapter notre processus d’évaluation d’un fournisseur ou d’une solution en infonuagique, nous utilisons la catégorisation des informations qui seront confiées à ce fournisseur.

Critère	Niveau	Exigences
Confidentialité	Information personnelle	Centre de données au Canada
Intégrité	Impacts académiques et institutionnels	Mécanismes de ségrégation des tâches
Disponibilité	Impacts académiques et institutionnels	Redondance des centres de données

Prochaines étapes

- Finaliser la classification en collaboration avec les fiduciaires
- Sensibilisation à une utilisation responsable des informations institutionnelles
- Validation des mesures de sécurité en place pour les informations les plus sensibles