Université de Montréal

LA CATÉGORISATION DES ACTIFS INFORMATIONNELS : L'EXPÉRIENCE DE L'UNIVERSITÉ DE MONTRÉAL

Diane Baillargeon

Présentée dans le cadre du 46e congrès annuel de l'Association des archivistes du Québec

Palais des congrès de Montréal 2 juin 2017

PLAN DE LA PRÉSENTATION

La catégorisation des actifs informationnels CAI : éléments théoriques

- Fondements et définition
- Principes et objectifs
- Portée

La catégorisation des actifs informationnels à l'Université de Montréal

- Contexte
- Démarche
- Outils
- Bilan de l'opération 2011-2013
- Suites
- Bilan de l'opération 205-2016

LA CATÉGORISATION DES ACTIFS INFORMATIONNELS : ÉLÉMENTS THÉORIQUES

46e congrès de l'AAQ 2 juin 2017

Université de Montréal

Fondements légaux

- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q., c. G-103)
- Directive sur la sécurité de l'information gouvernementale
- Cadre gouvernemental de gestion de la sécurité de l'information

CAI FONDEMENTS ET DÉFINITION

Fondement gestion des risques

- Identification des risques potentiels risques inhérents
  - Vraisemblance du risque
  - Conséquence du risque
  - Vélocité du risque
  - Efficacité des mesures de traitement
- Évaluation du risque résiduel
- Détermination du niveau de risque acceptable
- Mise en œuvre des moyens de mitigation des risques

Fondements normatifs

- Famille des normes internationales ISO 27 000 sur les Systèmes de Management de la Sécurité de l'Information (SMSI) qui vise à :
  - aider les organisation de tous types et de toutes taille à gérer efficacement leur SMSI
  - assurer la sécurité de l'information vue comme un actif pour l'organisation
- COBIT 5 un référentiel utilisé par les entreprises et les professionnels en sécurité de l'information

CAI PROVENANCE ET DÉFINITION

Actif informationnel :

- Savoir ou donnée représentant de la valeur pour l'organisation
  - Information sur quelque support qu'elle se trouve
    - Tous les types de documents produits ou reçus
    - Données transitant sur les systèmes d'information
  - Actifs physiques : ordinateurs
  - Systèmes d'information : y compris les logiciels
  - Système de transmission de l'information : courriel
  - Actifs plus intangibles : réputation ou l'image de l'organisation

CAI PROVENANCE ET DÉFINITION

Catégorisation:

- Évaluation de la valeur des actifs informationnels en fonction :
  - Des obligations de l'organisation
  - De l'importance de l'information
  - De l'impact d'un dysfonctionnement pour l'organisation

CAI – PRINCIPES ET OBJECTIFS

S’appuie sur les principes suivants :

- Sensibilisation à la sécurité de l’information
- Attribution de responsabilités liées à la sécurité de l’information
- Évaluation des niveaux acceptables de risques
- Prévention active et détection des incidents liés à la sécurité de l’information
- Réexamen continu de la sécurité de l’information et modification des mesures de mitigation mises en place

CAI PRINCIPES ET OBJECTIFS

Inventorier les actifs informationnel les plus critiques pour l'organisation

Identifier les impacts qu'entraîneraient une perte de l'actif informationnel pour l'organisation

Évaluer le degré de protection nécessaire pour minimiser ce risque

Déterminer les priorités en matière de protection de l'information :

- En fonction de la valeur de l'actif informationnel en fonction des exigences légales, de sa sensibilité et de son importance critique pour l'organisation

CAI – PORTÉE

Sécurité de l'information

- Intégrité
- Confidentialité
- Disponibilité
- Non-répudiation ou imputation
- Authentification

CAI – PORTÉE

DIC

- Disponibilité de l'information
  - Information atteignable et utilisable en temps voulu et de la manière adéquate par une personne autorisée
- Intégrité de l'information
  - Information qui n'est ni modifiée, ni altérée, ni détruite sans autorisation
- Confidentialité de l'information
  - Information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées

LA CATÉGORISATION DES ACTIFS INFORMATIONNELS À L'UNIVERSITÉ DE MONTRÉAL

46e congrès de l'AAQ

2 juin 2017

Université de Montréal

LA CAI À L'UNIVERSITÉ DE MONTRÉAL - CONTEXTE

- Recommandation du comité de vérification
  - Compléter la *Politique sur la protection des renseignements personnels*
  - Adopter les meilleures pratiques en la matière
  - Complémenter les démarches de performance organisationnelle et gestion des risques et de
  - Continuité des affaires

Contexte de discussion autour d'une nouvelle offre de services pour l'augmentation des espaces de stockage en infonuagique

LA CAI À L'UNIVERSITÉ DE MONTRÉAL - DÉMARCHE

Doter l'Université d'une Politique sur la gestion de l'information

- Applicable et devant s'inscrire dans une perspective globale
- Élaborer un cadre d'application découlant de la politique adoptée
- Établir une catégorisation des actifs informationnels

Formation d'un groupe de travail

- DGDA responsable
- Bureau du Registraire, DGTIC, Direction prévention et sécurité, Professeur DIRO,

Processus de catégorisation des actifs

- Inventaire des processus d'affaires
- Processus d'affaires :
  - Ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie. (Norme ISO9000:2000)
  - Plan de classification SOC 2
  - Calendrier de conservation des documents

CAI À L'UNIVERSITÉ DE MONTRÉAL - DÉMARCHE

- Matrice permet de voir d'un coup d'œil l'ensemble des processus d'affaires
  - Processus d'affaire donne lieu à la création de différents types de documents
- Détermination de seuils de criticité pour chaque critère
  - Évaluer de 1 à 3 du moins critique au plus critique
  - Élaboration d'une matrice rassemblant les informations

Disponibilité

- Niveau 1
  - Peut être acceptable que l'information ne soit pas disponible pendant une période prolongée (panne ou inaccessibilité de plus de 48 heures).
- Niveau 2
  - Période de non-disponibilité de l'information peut être tolérée mais pose des problèmes sans toutefois nuire à la mission de l'Université (panne ou inaccessibilité de moins de 48 heures)..
- Niveau 3
  - Courte période d'inaccessibilité tolérable (inférieure à 4 heures). Au-delà de cette période, la mission de l'Université peut être compromise

Unité administrative	Processus d'affaires	Détenteur	Documents ou groupes de documents	Systèmes d'information	Localisation (serveurs / composantes)	Intrant	Extrant	Gestion centralisée (O ou N)	Type de document		Seuils d'impact			Processus sélectionné	Date de création /MAJ
									Papier	Électronique	D	I	C		
	02 Affaires étudiantes (scolarité)														
	02.01 Clientèle étudiante														
Bureau de l'admission et du recrutement	02.01.01 Prévisions										1	2	2		
Bureau de l'admission et du recrutement	02.01.02 Recrutement										1	2	2		
Registrariat	02.01.03 Effectifs étudiants										3	3	2		
Registrariat	02.02 Admission										3	3	2		

CAI À L'UNIVERSITÉ DE MONTRÉAL - OUTILS

- Désignation d'un répondant par unité
- Session d'information aux répondants
- Validation des seuils d'impact par les répondants
- Doit être fait avec des personnes ayant une connaissance réel des processus d'affaire et capable d'évaluer les impacts

Nombre de matrices envoyées

- 15 facultés
- 24 services administratifs

Nombre de matrices retournées avec commentaires

- 10 facultés
- 20 services
- 26 départements
- 23 centres de recherche

Cotes attribuées par le comité étaient à 80% inchangées

CAI À L'UNIVERSITÉ DE MONTRÉAL – BILAN 2013

Série	Nombre	Retenus	Non retenus
1 - Enseignement	8	2	6
2- Affaires étudiantes	7	6	1
3 - Recherche	5	2	3
4 - Coopération	3	0	3
5 - Services à la communauté	28	9	19
6 - Administration	6	2	4
7 - Comités et autres organismes	7	1	6
8 - Personnel	13	4	9
9 - Finances	8	5	3
10 - Immeubles , mobilieres et équipements	5	1	4
11- Ressources informationnelles	14	2	12
12 - Communications	7	0	7
Total	**111**	**34**	**77**
%		31%	69%

CAI À L'UNIVERSITÉ DE MONTRÉAL – BILAN

- Janvier 2013, adoption d'une ***Politique sur la gestion de l'information*** *(*10.47*)*

- Création d'un ***Comité sur la gestion de l'information*** dont le mandat inclut l'élaboration et la mise à jour aux deux ans d'un catégorisation des actifs informationnels

- Septembre 2013, adoption de la première version de la ***Catégorisation des actifs informationnels***

Entre 2013 et 2016

- Visites d'unités pour évaluer le traitement des actifs numériques et papier découlant de processus critiques
- Bilan servi à alimenter la colonne sécurité pour le numérique (espace de stockage) et le papier (rangement, transmission, élimination)

Leçons apprises

- Tout prend beaucoup plus de temps que prévu
- Quantité de matrices retournées intéressantes, mais manque des unités importantes
- Peu de changements : parce que tout est bon ou parce que les responsables n'ont pas accordée l'attention nécessaire ?
- Important était d'identifier les séries critiques
- Compétence plus au niveau de la confidentialité
- Trouver des alliées pour les valeurs liés à la disponibilité et l'intégrité

Leçons apprises

- Donne une grande visibilité à la DGDA
- Donne une grande crédibilité à la DGDA
- Donner lieu à des applications concrètes
    - Directive sur l'infonuagique
    - Règles de gestion
    - Participation de la DGDA au Comité sur la gestion de l'information et aux ateliers de gestion des risques de projets structurants
    - Nouveaux alliés qui ont du poids

La catégorisation des actifs informationnels sert maintenant de base :

- Plan de travail du Bureau de la vérification interne
- Principes guidant la directive concernant le stockage de l'information institutionnelle en infonuagique (10.54)
- Colonne sécurité des règles de gestion
- Élément porteur et structurant pour la sécurité de l'information à l'Université de Montréal

Catégorisation des actifs a fait l'objet d'une révision en 2016

- Basée sur la nouvelle structure de cotation
- Catégorisation ramenée aux classes extrêmes de la structure de classification
- Permis de raffiner les cotes de criticité
- Mise à jour n'a pas modifiée la proportion des séries critiques et non critiques

Leçons apprises

- Archivistes possèdent une expertise dans l'évaluation des actifs informationnels que nous sous-estimons
- Cette expertise est reconnue par les membres de la communauté universitaire
- Cette reconnaissance et cette confiance sont précieuses, soyons-en fiers et servons-nous en!

Questions ?