Université du Québec

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

Catégorisation des actifs basée sur l'approche par l'analyse des préjudices – CESI

Université du Québec

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE OF CONTENTS

INTRODUCTION

CONTEXTE

L'information constitue une ressource essentielle qui doit être protégée tout au long de son cycle de vie, raison pour laquelle il est primordial de garder à jour l'inventaire de l'ensemble des actifs informationnels de l'organisation. L'un des premiers intrants de la sécurité de l'information est la connaissance de la sensibilité de l'information des actifs informationnels d'une organisation, en particulier, d'un établissement de l'Université du Québec.

Plusieurs méthodes permettent de déterminer cette sensibilité : c'est-à-dire : non sensible, sensible ou très sensible. Pour soutenir les organismes publics dans cette démarche, le Secrétariat du Conseil du Trésor (SCT) a élaboré en 2016 un guide basé sur la méthode de catégorisation des actifs informationnels. Bien que cette méthode ait permis aux établissements d'identifier la sensibilité de leur information, il n'en demeure pas moins que les résultats des exercices de celle-ci diffèrent d'un établissement à l'autre pour un actif corporatif qui manipule et traite les mêmes informations.

L'une des conséquences est la mise en œuvre de mesures de sécurité différentes pour assurer la protection de l'actif. Ainsi, un établissement X peut considérer l'actif A non sensible et le protéger avec des mesures de sécurité moindre, alors que l'établissement Y considèrera le même actif A comme très sensible et mettra en place plus de mesure de sécurité pour sa protection. Cette situation a conduit le Centre d'expertise en sécurité de l'information (CESI) à identifier une approche lui permettant d'obtenir des résultats consensuels et harmonisés.

OBJECTIF DU DOCUMENT

Le présent document vise à expliquer la nécessité d'effectuer la catégorisation des actifs informationnels et décrit de manière explicite la méthode d'analyse des préjudices, qui est une autre méthode de catégorisation répondant au mieux aux besoins des établissements de d'enseignement supérieur.

PORTÉE

Ce document s'adresse à tous les établissements d'enseignement supérieur, aux détenteurs de l'information, aux responsables, aux professionnels de la sécurité de l'information et à toutes les ressources qui seront sollicitées dans la démarche d'analyse des préjudices.

OBJECTIFS DE LA CATÉGORISATION

Ce guide fournit un aperçu complet de la catégorisation des actifs basée sur l'approche par l'analyse des préjudices, et ayant pour objectif d'aider les établissements à comprendre son fonctionnement et sa place, dans un programme de sécurité pour protéger la confidentialité, l'intégrité et la confidentialité des données des établissements de l'Université de Québec.

CATÉGORISATION DES ACTIFS INFORMATIONNELS

QU'EST-CE QUE LA CATÉGORISATION DES ACTIFS INFORMATIONNELS

Conformément au guide de catégorisation de l'information développé par le SCT, la catégorisation des actifs informationnels en sécurité de l'information se définit comme un processus permettant à un établissement d'évaluer le niveau de sensibilité de son information en matière de disponibilité, d'intégrité et de confidentialité (DIC), dans le but d'en déterminer le niveau de protection eu égard aux risques encourus en matière de disponibilité.

Ce niveau de sensibilité permet de choisir adéquatement les contrôles à adapter pour mieux protéger les actifs informationnels. Par exemple, un établissement pourra ainsi tenir compte du degré de sensibilité déterminé pour mettre en place les mesures lui permettant de se conformer à ses obligations légales, d'éviter des pertes financières, une atteinte à la réputation et d'atteindre ses objectifs en ce qui a trait à son niveau de services, ce qui aura pour conséquence de rehausser la confiance des citoyens et des entreprises à l'égard des services publics.

Lorsqu'elle est bien faite, la catégorisation des données rend la protection de celles-ci plus efficace. Pourtant, la catégorisation est souvent négligée, en particulier lorsque les établissements ne comprennent pas pleinement son objectif, sa portée et ses capacités.

La catégorisation des actifs diffère de l'analyse des risques basée sur les actifs. Après l'analyse de ceux-ci, nous allons considérer la catégorisation sur l'analyse des préjudices et des éléments qui pourraient les affecter (vulnérabilités et menaces).

RÉVISION DE LA CATÉGORISATION

Il est important de réévaluer la catégorisation des actifs informationnels sur une base périodique pour s'assurer que la catégorisation attribuée est toujours appropriée en fonction des modifications des obligations légales et contractuelles, ainsi que des changements dans l'utilisation des données ou leur valeur pour l'établissement. Cette évaluation devrait être effectuée par le détenteur de l'actif.

Le CESI encourage fortement que la révision de la catégorisation des actifs se fasse sur une base annuelle et encourage tous les établissements de l'Université de Québec à mettre en place un processus, afin que la révision des actifs se fasse effectivement à la fréquence choisie par chaque établissement. Cependant, le détenteur de l'actif informationnel a la décision finale de déterminer la fréquence la plus appropriée en fonction des ressources disponibles.

Si un détenteur détermine que la catégorisation d'un certain ensemble de données a changé, une analyse des contrôles de sécurité doit être effectuée pour déterminer si les contrôles existants sont conformes avec la nouvelle catégorisation. Si des insuffisances sont découvertes dans les contrôles de sécurité existants, elles doivent être corrigées en temps opportun et en fonction du niveau de risque présenté par les déficiences.

QUI EST RESPONSABLE DE LA CATÉGORISATION

La catégorisation d'un actif informationnel devrait être effectuée par le détenteur de l'actif, qui est en général le gestionnaire de l'unité d'affaires responsable de l'actif, et ce, en collaboration avec l'équipe de la sécurité des TI.

En effet, le détenteur de l'actif possède généralement une connaissance adéquate des impacts d'affaires advenant une perte de disponibilité, d'intégrité et de confidentialité de cet actif. Également, il connait les lois et réglementations assujetties à l'information de l'actif (ex. : Loi sur la protection des renseignements personnels, PCI-DSS, etc.) ainsi que les conséquences d'y contrevenir.

Afin de réaliser la catégorisation des actifs, la haute direction de l'établissement devra désigner un responsable, fournir les ressources requises à la réalisation de ce projet et communiquer formellement son appui. En effet, des efforts non négligeables devront être consentis pour mener à terme ce projet. Notamment, les détenteurs et gestionnaires de l'entreprise devront être mis à contribution afin de décrire les processus de leur unité d'affaires et de ressortir les différentes informations (ou familles d'information) qui y sont exploitées (incluant les intrants, les extrants, l'endroit où se trouve l'information, etc.). Par la suite, ces gestionnaires pourront attribuer les cotes d'impacts pertinentes aux actifs dont ils sont propriétaires.

POURQUOI CATÉGORISER LES DONNÉES

La confidentialité, l'intégrité et la disponibilité des actifs deviennent très difficiles à protéger si les établissements n'ont pas un inventaire de tous leurs actifs, mais aussi s'ils ne connaissent pas leur sensibilité, y compris où ils se trouvent.

Selon *Forrester*, les professionnels de la sécurité de l'information ne peuvent pas protéger efficacement les informations des clients, des employés et de l'organisation s'ils ne connaissent pas les éléments suivants :

- Quelles données existent dans leur organisation;
- Où elle réside exactement;
- Leur valeur et leur risque pour l'organisation;
- Règles de conformité régissant les données;
- Qui est autorisé à accéder aux données et à les utiliser.

https://www.spirion.com/data-classification/#:~:text=According%20to%20Forrester%2C%20data%20privacy,data%20exists%20across%20their%20enterprise

D'autre part, comme on peut le voir ci-dessous, la catégorisation permet de mener plusieurs activités importantes en matière de sécurité de l'information.

Figure 1 : Exemples de cas d'utilisation des résultats du processus de catégorisation
Référence : Guide de catégorisation de l'information – Version 2.1

EXEMPLES DE DESCRIPTION DES RÉSULTATS DE LA CATÉGORISATION

- Le choix du fournisseur infonuagique doit être fait en vue d'assurer la protection des actifs informationnels selon leur sensibilité;
- L'élaboration des plans d'action de sécurité de l'information permet à l'organisation d'accorder une plus grande priorité aux actifs informationnels importants pour l'organisme;
- L'audit de sécurité permet de s'assurer de l'adéquation des mesures de sécurité mise en place par rapport au niveau de criticité des actifs informationnels;
- La mise en œuvre de stratégies de continuité des services, axées sur les actifs informationnels à valeur élevée;
- La formation et la sensibilisation des employés et des partenaires aux mesures de protection associées à la valeur de l'information utilisée;
- La gestion des incidents de sécurité de l'information, en tenant compte du degré de sensibilité des actifs informationnels;
- Le choix du procédé de destruction sécuritaire de l'information, en tenant compte de la valeur de cette information;
- La mise en place de mécanismes de contrôle d'accès à l'information selon son niveau de sensibilité.

AVANTAGES DE LA CATÉGORISATION DES DONNÉES

Plusieurs organisations ont très peu de connaissance sur le portrait de leurs actifs informationnels, ce qui entraine une problématique sur leur protection. Il s'agit d'un problème sérieux dans la lutte pour assurer efficacement la confidentialité, l'intégrité et la disponibilité des données sensibles. En lançant des programmes de catégorisation des données complets et bien planifiés, les établissements bénéficient d'un large éventail d'avantages.

AMÉLIORER LA SÉCURITÉ DES DONNÉES

La catégorisation des données permet aux établissements de protéger les données sensibles de l'organisation et des clients, notamment :

- Réduire l'accès aux données sensibles aux seuls utilisateurs approuvés;
- Comprendre la criticité des différents types de données afin de mieux les protéger;
- Utiliser les bonnes technologies de protection des données, telles que le chiffrement, la prévention de la perte de données (DLP) et la perte et la protection de l'identité (ILP);
- Optimiser les coûts sans gaspiller de ressources sur des données non critiques ou moins critiques.

SOUTENIR LA CONFORMITÉ RÉGLEMENTAIRE

La catégorisation des actifs informationnels aide à déterminer où se trouvent les données réglementées dans l'établissement, garantit que des contrôles de sécurité appropriés sont en place et que les données sont traçables et consultables, comme l'exigent les réglementations de conformité. Cela offre ces avantages :

- S'assurer que les données sensibles sont traitées de manière appropriée pour différentes réglementations, telles que les informations médicales, de cartes de crédit et d'identification personnelle;
- Développer une capacité à maintenir la conformité quotidienne avec toutes les règles, réglementations et lois pertinentes sur la confidentialité;
- Prendre en charge la récupération rapide d'informations spécifiques dans un délai défini, ce qui permet de respecter les nouvelles règles de conformité;
- Démontre l'expertise des établissements et le soutien des programmes qui garantissent la conformité à la confidentialité des données;
- Améliore la possibilité de réussir les audits de conformité.

Quelques normes de conformité :

- DGSI

Directive gouvernementale sur la sécurité de l'information

- LGGRI

G-1.03 - Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement

- HIPAA

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- PCI DSS

Payment Card Industry Data Security Standard

AMÉLIORER L'EFFICACITÉ DES OPÉRATIONS ET RÉDUIRE LES RISQUES D'AFFAIRES

Depuis la création des informations jusqu'à leur destruction, la catégorisation des actifs peut aider les établissements à s'assurer qu'elles protègent, stockent et gèrent efficacement leurs données. Cela offre les avantages suivants :

- Fournis un meilleur aperçu et un meilleur contrôle des données que les établissements détiennent et partagent;
- Permets un accès et une utilisation plus efficaces des données protégées dans toute l'organisation;
- Facilite la gestion des risques en aidant les établissements à évaluer la valeur de leurs données et l'impact de leurs perte, vol, mauvaise utilisation ou compromis;
- Apporte des fonctionnalités précieuses pour la conservation des enregistrements et la découverte légale.

LA MÉTHODE D'ANALYSE DES PRÉJUDICES

La catégorisation de la sécurité est un processus qui permet d'identifier les possibles préjudices liés à la compromission des données d'un actif opérationnel. Les activités opérationnelles sont d'abord catégorisées d'après la détermination du préjudice prévu qui découle des menaces de compromission des TI, puis d'après la détermination du niveau de ce préjudice.

Dans le cadre de ce processus, les activités opérationnelles qui seront prises en charge par les services fondés sur l'infonuagique sont établies et classées par catégorie, et le service hérite de la catégorie de sécurité attribuée. Les clients de services infonuagiques choisissent alors le profil de contrôle de sécurité qui convient à la catégorie de sécurité et à leur tolérance au risque. La catégorie de sécurité est également l'un des facteurs pris en compte au moment de sélectionner les modèles de déploiement en nuage et de service infonuagique.

Une catégorie de sécurité exprime les niveaux les plus élevés de préjudices prévus qui découlent des menaces de compromission par rapport aux objectifs de sécurité liés à la confidentialité, l'intégrité et la disponibilité.

DÉFINITION D'UN PRÉJUDICE

Selon l'Office québécois de la langue française (OQLF), un préjudice signifie « perte, tort ou dommage causé par autrui » ou « acte, événement nuisible à quelque chose ou à quelqu'un ».

En sécurité de l'information, on entend par préjudices, un dommage engendré par une compromission d'un des objectifs sécurité (disponibilité, l'intégrité et la confidentialité) qui affecte directement les utilisateurs ou les bénéficiaires des services fournis par le gouvernement du Québec. En d'autres mots, le préjudice concerne la sécurité, la santé et le bien-être des personnes, ainsi que la situation financière et la réputation des personnes et des entreprises.

Par compromission, on entend une destruction, une suppression, une modification, une divulgation, ou un accès non autorisé à l'information, entraînant une perte de disponibilité, d'intégrité ou de confidentialité.

Voici quelque exemple de type de préjudices :

- La perte de réputation;
- L'atteinte à la vie privée;
- Des amendes pour infraction aux réglementations (gouvernementales);
- Les pénalités contractuelles (non-respect des contrats existants);
- La perte de revenus;
- La perte de vie.

Afin de faciliter et d'avoir une approche commune des préjudices dans les établissements de l'Université du Québec, un tableau de préjudice a été élaboré au paragraphe suivant.

TABLEAU DES PRÉJUDICES – TYPE ET NIVEAU DE PRÉJUDICES

Le tableau ci-dessous doit être utilisé pour identifier les préjudices applicables lors de la compromission des critères de sécurité.

Type de préjudices	Niveau				
	Très faible	**Faible**	**Modéré**	**Élevé**	**Très élevé**
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort physique	Douleur physique, blessure, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Stress	Détresse, traumatisme psychologique	Maladie ou trouble mental	Traumatisme psychologique généralisé
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort et stress causé	Qualité de vie affectée	Sécurité financière compromise	Sans objet
Perte financière pour des entreprises	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement	Réduction de la compétitivité	Viabilité compromise	Sans objet
Perte financière pour le gouvernement du Québec	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement du service	Incidence sur les résultats du service	Viabilité du service compromise	Viabilité des services essentiels compromise
Préjudice causé à l'économie québécoise	Sans objet	Sans objet	Incidence sur le rendement	Perte de la compétitivité à l'échelle internationale	Secteurs économiques clés compromis
Agitation ou désordre civil	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, obstruction publique	Émeute	Acte de sabotage à l'égard des biens essentiels (ex. : infrastructure essentielle)	Émeute générale ou acte de sabotage nécessitant l'imposition d'une loi martiale
Préjudice causé à la réputation du Québec	Préjudice négligeable ou aucun préjudice raisonnable prévu	Perte de la confiance du public	Embarras (au Québec ou à l'étranger)	Dommage aux relations avec les autres provinces	Relations diplomatiques et internationales compromises
Perte de l'autonomie du Québec	Sans objet	Sans objet	Entrave à l'établissement de politiques gouvernementales importante	Entrave à l'application efficace de la loi, cessation des activités du gouvernement	Sans objet

Figure 2 : tableau de la liste des préjudices

Référence : Programme de Consolidation des CTI - Guide d'analyse des préjudices de sécurité

DÉMARCHE ORGANISATIONNELLE POUR LA CATÉGORISATION DES ACTIFS D'UN ÉTABLISSEMENT

La catégorisation des actifs d'un établissement doit suivre la démarche suivante :

EXEMPLE D'UN PROCESSUS DE CATÉGORISATION BASÉE SUR L'ANALYSE DE PRÉJUDICE

Afin d'encourager les études, le gouvernement a mis en place un programme nommé « prêts et bourses » dirigé par un département du ministère de l'Enseignement. Le programme de prêts et bourse a pour objectif de réceptionner les demandes d'ouverture de dossier, analyser les demandes et calculer le montant de prêts et bourse à octroyer au demandeur.
Ce programme est supporté par trois processus opérationnels :

1. Ouverture du dossier de prêts et bourse

Ce processus opérationnel comprend deux composantes :

- Réception de la demande et ouverture du dossier : c'est un processus qui consiste à recevoir la demande et à créer le dossier du demandeur;
- Renseignements personnels du demandeur : Les renseignements concernent les informations personnelles du requérant (NAS, date de naissance, adresse, etc.), sa situation financière (revenu d'emploi, etc.), quelques informations relatives à ses parents et à sa situation matrimoniale (enfants à charge, etc.), et des informations sur le programme de formation et l'établissement de formation (CÉGEP, Université, etc.).

2. Examen du dossier de prêts et bourse

Ce processus opérationnel comprend une seule composante :

- Approbation du montant du prêt et bourse : une analyse du dossier permet de fixer le montant à verser à partir de barèmes prédéfinis. La banque du requérant reçoit l'ordre de virement pour la période (session ayant fait l'objet de la demande de prêt et bourse) sollicitée. La même banque responsable du recouvrement des prêts lorsque le gouvernement le demande généralement après l'obtention du diplôme.

3. Service de paiement de prêts et bourse

Ce processus opérationnel comprend une seule composante :

- Versement du montant du montant du prêt et bourse : la banque du demandeur reçoit l'ordre de virement pour la période (session ayant fait l'objet de la demande de prêt et bourse) sollicitée. La même banque est responsable du recouvrement des prêts lorsque le gouvernement le demande généralement après l'obtention du diplôme.

INVENTAIRE DES ACTIFS

L'analyse des préjudices peut concerner un nouveau projet, un processus d'affaires, des services du processus d'affaires, des activités opérationnelles et des systèmes d'information qui le supportent. Ceci fait en sorte que le niveau de découpage des informations (par processus d'affaires ou par service, etc.,) est très important.

NIVEAU DE GRANULARITÉ DE L'INVENTAIRE POUR LA CATÉGORISATION

Le niveau de granularité est le degré de détail recherché lors de l'identification des objets à catégoriser. Le niveau de détail de l'information est généralement défini par son propriétaire ou par une instance de sécurité. La détermination du niveau de détail de l'inventaire est un des enjeux associés au processus d'inventaire.

Dans le cas de vastes organisations comportant plusieurs programmes, on ne peut effectuer l'inventaire des processus opérationnels et des composantes de ces processus opérationnels qu'en le divisant en programme, en sous-programme ou en sous-sous-programme. Il est ainsi possible d'offrir à ces organisations le niveau de détail nécessaire pour établir les exigences de sécurité tant au niveau de la composante du processus opérationnel qu'au niveau du programme. Cela aura aussi pour objectif final de ne pas par exemple envoyer dans le nuage, des sous-programmes d'un processus opérationnel qui ne sont pas sensible.

ÉLÉMENT D'IDENTIFICATION DE L'ACTIF INFORMATIONNEL

Quel que soit le niveau de granularité souhaité lors de l'inventaire, chacun des actifs est caractérisé par les éléments suivants :

- Nom de l'objet de catégorisation;
- Nom du processus opérationnel;
- La ou les composante(s) du processus opérationnel (services);
- Description de la ou les composante(s) du processus opérationnel (services);
- Type objet.

Objet de catégorisation	Processus operationnel	Composante du processus operationnel	Description de la composante	Type objet
Prets et Bourse	Ouverture du dossier de prêts et bourse	Réception de la demande et ouverture du dossier	Processus qui consiste à recevoir la demande et à créer le dossier du demandeur	Electronique/papier
		Renseignements personnels du demandeur	Nom, adresse, numéros de téléphone, information concernant les membres de la famille, numéro d'assurance sociale, informations bancaires (pour le dépôt direct)	Electronique/papier
	Examen du dossier de prêts et bourse	Approbation du montant du prêt et bourse	Processus qui consiste à analyser la demande et à fixer le montant à verser	Electronique
	Service de paiement de prêts et bourse	Versement du montant du montant du prêt et bourse	Processus qui consiste à envoyer l'ordre de virement du montant du pret et bourse pour la session a la banque du demandeur	Electronique

Figure 3 : Tableau de l'inventaire des actifs de l'objet de catégorisation – Prêts et Bourse

FORMATION DU COMITÉ POUR L'ÉVALUATION DES PRÉJUDICES

Le processus d'évaluation du préjudice devrait être confié à des équipes composées de représentants des secteurs responsables des opérations, des questions juridiques, de l'accès à l'information, de la sécurité et du respect de la vie privée. Le détenteur ou son délégué devrait également faire partie de ces équipes, de même que le responsable de l'autorisation (si cette tâche n'a pas été confiée au propriétaire opérationnel) et les représentants et analystes opérationnels de chaque programme ou secteur d'activités. Dans la présente, on désigne ce groupe par le nom collectif « comité d'évaluation ».

Voici quelque compétence nécessaire à la réalisation de l'analyse des préjudices :

- Pilote du système évalué;
- Conseiller en sécurité;
- Utilisateur du système;
- Architecte d'affaires;
- Détenteur ou son représentant.

ÉVALUATION DES PRÉJUDICES

L'objectif de l'évaluation du préjudice est de déterminer le préjudice prévu lié aux menaces de compromission pour chaque processus opérationnel et chaque bien d'information déterminé à l'étape précédente). Idéalement, les universités doivent évaluer les préjudices associés à leurs processus opérationnels et aux biens d'information connexes en recourant à un processus auquel participent des équipes multidisciplinaires qui regroupent des représentants des domaines opérationnels, juridiques, de l'accès à l'information et du respect de la vie privée.

La réussite de l'évaluation des préjudices prend en compte la démarche suivante :

1. **Le scénario de compromission ou de défaillance** : C'est la description des évènements pouvant engendrer des préjudices si les critères de sécurité du système étaient compromis;
2. **Type et niveau de préjudice** : Choisir le préjudice (cellule) applicable dans le tableau de préjudices;
3. **Facteurs spéciaux** : La prise en compte de certains éléments pourrait influencer sur les préjudices;
4. **Analyse** : justification du choix, argumentaire, observation.

Il est à noter que les quatre étapes de l'évaluation de préjudice ci-dessus sont effectuées par rapport à chaque objectif de sécurité de l'information (Disponibilité, intégrité et confidentialité).

DETERMINATION DU SCÉNARIO DE COMPROMISSION

Comme le titre l'indique, il s'agit de trouver des scénarios réalistes qui pourraient compromettre la disponibilité, l'intégrité et la confidentialité de l'actif. La détermination des scénarios de défaillance vise à tenir compte des différentes façons dont une composante peut faire l'objet d'une défaillance et causer un préjudice. Notez que plus d'un scénario de défaillance peut être attribué à chacune des composantes d'une activité opérationnelle.

Objet de catégorisation	Processus operationnel	Composante du processus operationnel	Description de la composante	Type objet	Scénario de compromission		
					D	I	C
Prets et Bourse	Ouverture du dossier de prêts et bourse	Réception de la demande et ouverture du dossier	Processus qui consiste à recevoir la demande et à créer le dossier du demandeur	Electronique/papier	Le service de réception de la demande et ouverture du dossier n'est pas accessible pendant 48 heures	S.O	S,O
		Renseignements personnels du demandeur	Nom, adresse, numéros de téléphone, information concernant les membres de la famille, numéro d'assurance sociale, informations bancaires (pour le dépôt direct)	Electronique/papier	Les renseignements personnels du demandeur ne figure pas sur la demande	Corruption des données par rançongiciel	Divulgation d'information personnelle (dont le NAS) à une personne non autorisée aux intentions malveillantes
	Examen du dossier de prêts et bourse	Approbation du montant du prêt et bourse	Processus qui consiste à analyser la demande et à fixer le montant à verser	Electronique	Le service ou la personne responsible de l'approbation du montant du pret n'est pas disponible pendant 48 heures	Erreur sur le montant fixé pour le prêt et bourse	Divulgation du montant du pret et bourse
	Service de paiement de prêts et bourse	Versement du montant du montant du prêt et bourse	Processus qui consiste à envoyer l'ordre de virement du montant du pret et bourse pour la session a la banque du demandeur	Electronique	L'ordre de virement du montant du pret et bourse pour la session a la banque du demandeur n'est pas disponible pendant 48 heures	Erreur sur le montant du prêt et bourse versé par la banque au demandeur	Divulgation du montant du pret et bourse versé par la banaque au demandeur

Figure 4 : Tableau de description des différents scénarios de compromission de l'objet de catégorisation – Prêts et Bourse

TYPE ET NIVEAU DE PRÉJUDICES

Le comité d'évaluation doit utiliser le tableau de préjudices en vue de déterminer le niveau possible de préjudice des actifs informationnels. En d'autres termes, la détermination du niveau de préjudice associé à un actif d'un processus d'affaires se fait de la façon suivante :

1. La sélection du type de préjudice associé au scénario de compromission (axe vertical du tableau des préjudices);
2. La sélection, dans le tableau de l'exemple de préjudice qui représente le plus fidèlement l'évaluation de ce qui risque de se produire pendant la réalisation du scénario;
3. La sélection dans l'axe horizontal du niveau de préjudice associé à l'exemple de préjudice choisi dans le tableau des préjudices.

LES FACTEURS SPÉCIAUX INFLUENÇANT LES PRÉJUDICES

Au cours de l'évaluation des préjudices, les praticiens de la sécurité doivent tenir compte de plusieurs facteurs susceptibles d'influer sur les résultats, incluant les suivants :

AGRÉGATION DE L'INFORMATION

Lorsqu'un objet de catégorisation contient des éléments de niveaux d'impact différents, c'est généralement le niveau le plus élevé qui l'emporte. Ainsi, un processus impliquant plusieurs actifs informationnels de niveaux d'impact différents peut être considéré comme une agrégation de ces actifs et hériter du niveau d'impact le plus élevé. De même, un objet de catégorisation peut hériter d'un niveau d'impact supérieur à ceux attribués individuellement aux actifs informationnels qui le composent.

LE TEMPS

La catégorisation de certains actifs informationnels est sensible au facteur « temps ». Un actif informationnel peut avoir un niveau de confidentialité élevé pour une période donnée et être public par la suite. Dans ce cas, il est recommandé de revoir la catégorisation de cet actif selon les étapes de son cycle de vie.

CAS : COMPOSANTE DU PROCESSUS OPÉRATIONNEL - RENSEIGNEMENTS PERSONNELS DU DEMANDEUR

ANALYSE DE LA SENSIBILITÉ AU NIVEAU DE LA DISPONIBILITÉ

Scénario de compromission : Indisponibilité des renseignements personnels du demandeur de plus de 48h;

Question : Quels seraient les préjudices directs, pour la personne elle-même, les entreprises ou le gouvernement si les renseignements personnels du demandeur ne figuraient pas sur la demande?

Type de préjudices	Très faible		Faible		Modéré		Élevé		Très élevé	
Préjudice physique causé aux personnes		Préjudice négligeable ou aucun préjudice raisonnable prévu		Inconfort physique		Douleur physique, blessure, traumatisme, difficultés, maladie		Incapacité physique, décès		Lourdes pertes de vie
Préjudice psychologique causé aux personnes		Préjudice négligeable ou aucun préjudice raisonnable prévu	x	Stress		Détresse, traumatisme psychologique		Maladie ou trouble mental		Traumatisme psychologique généralisé
Perte financière pour des particuliers		Préjudice négligeable ou aucun préjudice raisonnable prévu	x	Inconfort et stress causé		Qualité de vie affectée		Sécurité financière compromise		Sans Objet
Perte financière pour des entreprises		Préjudice négligeable ou aucun préjudice raisonnable prévu		Incidence sur le rendement		Réduction de la compétitivité		Viabilité compromise		Sans Objet
Perte financière pour le gouvernement du Québec		Préjudice négligeable ou aucun préjudice raisonnable prévu		Incidence sur le rendement du service / plus difficile d'atteindre les objectifs du gouvernement		Incidence sur les résultats du service / incapacité d'atteindre les objectifs du gouvernement		Viabilité du service compromise		Viabilité des services essentiels compromise
Préjudice causé à l'économie québécoise		Sans Objet		Sans Objet		Incidence sur le rendement (baisse du PIB, impact sur un secteur économique)		Perte de la compétitivité à l'échelle internationale		Secteurs économiques clés compromis
Agitation ou désordre civil		Préjudice négligeable ou aucun préjudice raisonnable prévu		Désobéissance civile, obstruction publique		Émeute		Acte de sabotage à l'égard des biens essentiels (ex. : infrastructure essentielle)		Émeute générale ou acte de sabotage nécessitant l'imposition d'une loi martiale
Préjudice causé à la réputation du Québec		Préjudice négligeable ou aucun préjudice raisonnable prévu		Perte de la confiance du public		Embarras/impacts significatifs au QC ou à l'étranger (ex.: faire annuler un projet de loi) Perte de		Dommage aux relations avec les autres provinces		Relations diplomatiques et internationales compromises
Perte de l'autonomie du Québec		Sans Objet		Sans Objet		Entrave à l'établissement de politiques gouvernementales importantes		Entrave à l'application efficace de la loi, cessation des activités du gouvernement		Sans Objet

Figure 5 : Tableau de l'analyse de la sensibilité au niveau de la disponibilité de la composante de la composante du processus opérationnel – Renseignements personnels du demandeur

Analyse : Ceci peut engendrer du stress pour le demandeur et aussi causer de l'inconfort, car le traitement de sa demande pourrait accuser un retard. Le programme de prêt et bourse le contactera afin qu'il ajoute les informations manquantes.

Le niveau de préjudice pour la disponibilité est de D=Faible

ANALYSE DE LA SENSIBILITÉ AU NIVEAU DE L'INTÉGRITÉ

Scénario de compromission : Corruption des données par rançongiciel;

Question : Quels seraient les préjudices directs, pour la personne elle-même, les entreprises ou le gouvernement si les informations contenues dans le système étaient partiellement ou complètement inexactes à la suite d'une modification non autorisée des informations collectées et inscrites?

Analyse : Dans ce scénario, un étudiant qui attend la décision sur les bourses et/ou prêts sera affecté par le stress, car la demande pourrait être retardée. Aussi, si les données sont corrompues, cela entrainera une perte de la confiance du public, mais n'affectera pas la viabilité du service dans la mesure où des mesures palliatives seront prises pour corriger les choses rapidement. Par exemple, accorder un montant forfaitaire à tout demandeur ou bénéficiaire (comme le cas de la PCU en temps de COVID-19). Lorsque la situation sera normale, des compensations vont avoir lieu pour corriger le tout. Ce qui fait que le préjudice retenu sera du stress et la qualité de vie affectée relativement à la perte financière. Ce scénario peut aussi engendrer une perte de la confiance du public envers l'Université du Québec si la population est informée de la situation.

Le niveau de préjudice pour l'intégrité est donc **I=Faible**

Type de préjudices	Très faible	Faible	Modéré	Élevé	Très élevé
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort physique	Douleur physique, blessure, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	x Stress	Détresse, traumatisme psychologique	Maladie ou trouble mental	Traumatisme psychologique généralisé
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort et stress causé	Qualité de vie affectée	Sécurité financière compromise	Sans Objet
Perte financière pour des entreprises	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement	Réduction de la compétitivité	Viabilité compromise	Sans Objet
Perte financière pour le gouvernement du Québec	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement du service / plus difficile d'atteindre les objectifs du gouvernement	Incidence sur les résultats du service / incapacité d'atteindre les objectifs du gouvernement	Viabilité du service compromise	Viabilité des services essentiels compromise
Préjudice causé à l'économie québécoise	Sans Objet	Sans Objet	Incidence sur le rendement (baisse du PIB, impact sur un secteur économique)	Perte de la compétitivité à l'échelle internationale	Secteurs économiques clés compromis
Agitation ou désordre civil	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, obstruction publique	Émeute	Acte de sabotage à l'égard des biens essentiels (ex. : infrastructure essentielle)	Émeute générale ou acte de sabotage nécessitant l'imposition d'une loi martiale
Préjudice causé à la réputation du Québec	Préjudice négligeable ou aucun préjudice raisonnable prévu	x Perte de la confiance du public	Embarras/impacts significatifs au QC ou à l'étranger (ex.: faire annuler un projet de loi) Perte de	Dommage aux relations avec les autres provinces	Relations diplomatiques et internationales compromises
Perte de l'autonomie du Québec	Sans Objet	Sans Objet	Entrave à l'établissement de politiques gouvernementales importantes	Entrave à l'application efficace de la loi, cessation des activités du gouvernement	Sans Objet

Figure 5 : Tableau de l'analyse de la sensibilité au niveau de l'intégrité de la composante de la composante du processus opérationnel – Renseignements personnels du demandeur

ANALYSE DE LA SENSIBILITÉ AU NIVEAU DE LA CONFIDENTIALITÉ

Scénario de compromission : Divulgation d'information personnelle (dont le NAS) à une personne non autorisée aux intentions malveillantes;

Question : Quels seraient les préjudices, pour la personne elle-même, les entreprises ou le gouvernement si les renseignements personnels ou confidentiels étaient communiqués à un tiers qui ne devait pas y avoir accès.

Type de préjudices	Très faible	Faible	Modéré	Élevé	Très élevé
Préjudice physique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort physique	Douleur physique, blessure, traumatisme, difficultés, maladie	Incapacité physique, décès	Lourdes pertes de vie
Préjudice psychologique causé aux personnes	Préjudice négligeable ou aucun préjudice raisonnable prévu	x Stress	Détresse, traumatisme psychologique	Maladie ou trouble mental	Traumatisme psychologique généralisé
Perte financière pour des particuliers	Préjudice négligeable ou aucun préjudice raisonnable prévu	Inconfort et stress causé	X Qualité de vie affectée	Sécurité financière compromise	Sans Objet
Perte financière pour des entreprises	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement	Réduction de la compétitivité	Viabilité compromise	Sans Objet
Perte financière pour le gouvernement du Québec	Préjudice négligeable ou aucun préjudice raisonnable prévu	Incidence sur le rendement du service / plus difficile d'atteindre les objectifs du gouvernement	Incidence sur les résultats du service / incapacité d'atteindre les objectifs du gouvernement	Viabilité du service compromise	Viabilité des services essentiels compromise
Préjudice causé à l'économie québécoise	Sans Objet	Sans Objet	Incidence sur le rendement (baisse du PIB, impact sur un secteur économique)	Perte de la compétitivité à l'échelle internationale	Secteurs économiques clés compromis
Agitation ou désordre civil	Préjudice négligeable ou aucun préjudice raisonnable prévu	Désobéissance civile, obstruction publique	Émeute	Acte de sabotage à l'égard des biens essentiels (ex. : infrastructure essentielle)	Émeute générale ou acte de sabotage nécessitant l'imposition d'une loi martiale
Préjudice causé à la réputation du Québec	Préjudice négligeable ou aucun préjudice raisonnable prévu	x Perte de la confiance du public	Embarras/impacts significatifs au QC ou à l'étranger (ex.: faire annuler un projet de loi) Perte de	Dommage aux relations avec les autres provinces	Relations diplomatiques et internationales compromises
Perte de l'autonomie du Québec	Sans Objet	Sans Objet	Entrave à l'établissement de politiques gouvernementales importantes	Entrave à l'application efficace de la loi, cessation des activités du gouvernement	Sans Objet

Figure 7 : tableau de l'analyse de la sensibilité au niveau de la confidentialité de la composante de la composante du processus opérationnel – Renseignements personnels du demandeur

Analyse : Dans ce scénario, les informations telles que le nom, le prénom, l'adresse, le NAS, le numéro de compte bancaire sont suffisantes pour exemple, effectuer une demande une carte de crédit au nom de la victime ou aussi connaitre avec exactitude le domicile de la victime. Nous sommes ici dans un cas de **qualité de vie affectée, détresse**, **inconfort et stress et perte de la confiance du public** comme préjudice.

Le niveau de préjudice pour la confidentialité est **C= Modéré**

En conclusion la catégorisation pour le cas du processus opérationnel: ouverture du dossier de prêts et bourse/Renseignement sur le demandeur est **Faible-Faible- Modéré**

Le même exercice devra être répété pour tous les processus opérationnels du programme *Prêts et Bourse.*

FORMULAIRE DE VALIDATION DES RÉSULTATS DE LA CATÉGORISATION

Une fois l'évaluation des préjudices terminée, il est recommandé que le comité d'évaluation produise un rapport final de la catégorisation des actifs basée sur l'approche par l'analyse des préjudices pour communiquer les résultats.

Le Comité d'évaluation devrait documenter et accepter formellement les résultats de l'activité de catégorisation de la sécurité

Université	[A completer]
Equipe de validation	[A completer]
Date de validation	[A completer]
Detenteur	[A completer]
Date de catégorisation (jj/mm/aaaa)	[A completer]

Objet de catégorisation	Processus operationnel	Composante du processus operationnel	Description de la composante	Type objet	Scénario de compromission			Niveau de Prejudice			Niveau de sensibilité
					D	I	C	D	I	C	
Prets et Bourse	Ouverture du dossier de prêts et bourse	Réception de la demande et ouverture du dossier	Processus qui consiste à recevoir la demande et à créer le dossier du demandeur	Electronique/papier	Le service de réception de la demande et ouverture du dossier n'est pas accessible pendant 48 heures	S.O	S,O	Faible	Faible	Faible	Faible-Faible-Faible
		Renseignements personnels du demandeur	Nom, adresse, numéros de téléphone, information concernant les membres de la famille, numéro d'assurance sociale, informations bancaires (pour le dépôt direct)	Electronique/papier	Les renseignements personnels du demandeur ne figure pas sur la demande	Corruption des données par rançongiciel	Divulgation d'information personnelle (dont le NAS) à une personne non autorisée aux intentions malveillantes	Faible	Faible	Modéré	Faible-Faible-Modéré
	Examen du dossier de prêts et bourse	Approbation du montant du prêt et bourse	Processus qui consiste à analyser la demande et à fixer le montant à verser	Electronique	Le service ou la personne responsible de l'approbation du montant du pret n'est pas disponible pendant 48 heures	Erreur sur le montant fixé pour le prêt et bourse	Divulgation du montant du pret et bourse	Faible	Faible	Faible	Faible-Faible-Faible
	Service de paiement de prêts et bourse	Versement du montant du prêt et bourse	Processus qui consiste à envoyer l'ordre de virement du montant du pret et bourse pour la session a la banque du demandeur	Electronique	L'ordre de virement du montant du pret et bourse pour la session a la banque du demandeur n'est pas disponible pendant 48 heures	Erreur sur le montant du prêt et bourse versé par la banque au demandeur	Divulgation du montant du pret et bourse versé par la banaque au demandeur	Faible	Faible	Faible	Faible-Faible-Faible

Figure 8 : Tableau de validation des résultats de la catégorisation de l'objet de catégorisation – Prêts et Bourse

RAPPORT GLOBAL DE LA CATÉGORISATION DE L'OBJET DE CATÉGORISATION: PRÊTS ET BOURSE

Si tous les processus opérationnels sont pris en charge par un seul objet de catégorisation tel qu'illustré dans notre exemple alors, on pourrait utiliser, la catégorie globale qui correspond à la valeur maximale c'est-à-dire le niveau le plus élevé de préjudice dans chacune des colonnes du formulaire de validation des résultats de la catégorisation.

Objet de catégorisation	Disponibilité	Intégrité	Confidentialité
Programme de prêt et bourse	**Faible**	**Faible**	**Modéré**

Figure 9 : Tableau du rapport global de la catégorisation de l'objet de catégorisation – Prêts et Bourse

AVANTAGES ET INCONVÉNIENTS DE LA CATÉGORISATION GLOBALE

AVANTAGE

En règle générale, la meilleure approche consiste à attribuer une valeur maximale à un objet de catégorisation si l'objectif est de regrouper différents rapports de catégorisation. Cela a pour bénéfice de pouvoir choisir un seul profil de contrôles de sécurité qui sera appliqué à tous les processus opérationnels du domaine.

INCONVÉNIENTS

Cependant, le fait d'attribuer la valeur maximale au niveau de catégorisation sous-entend qu'on devra choisir et ajuster des contrôles ayant un coût plus élevé que la valeur de l'actif. Généralement, il n'est pas recommandé que le coût de l'implémentation des contrôles dépasse le coût de la valeur de l'actif informationnel. La décision ultime de regrouper les différents rapports de catégorisation revient à la haute direction.

ANALYSE DE PRÉJUDICES COMPARÉE À L'ANALYSE DE RISQUE

L'analyse du préjudice est une sous étape de l'analyse de risque. Elle fait partie de la phase d'identification et d'évaluation des actifs, définie dans la méthodologie harmonisée d'évaluation des menaces et des risques qui a été conçue par la Gendarmerie royale du Canada (GRC/RCMP) et le Centre de la Sécurité des Télécommunications (CST/CSE).

Les trois grandes phases de l'analyse de risque :

LA PHASE D'IDENTIFICATION ET D'ÉVALUATION DES ACTIFS

Cette phase comprend trois processus :

- **Identification des actifs** : consiste à dresser la liste de tous les actifs qui sont inclus dans la portée de l'évaluation à un niveau approprié de détail.
- **Évaluation des préjudices** : consiste à déterminer le préjudice qui pourrait vraisemblablement résulter d'une atteinte à la confidentialité, à la disponibilité ou à l'intégrité de chaque actif.
- Évaluation des actifs : consiste à attribuer une valeur à chaque actif sur les plans de la confidentialité, de la disponibilité et de l'intégrité, selon le cas, en se fondant sur des critères de préjudice courants.

LA PHASE D'ÉVALUATION DES MENACES

Cette phase comprend quatre processus :

- Identification des menaces : consiste à produire une liste de toutes les menaces susceptibles d'avoir une incidence sur les actifs prévus dans la portée de l'évaluation.
- Évaluation de la probabilité: consiste à évaluer la probabilité que chaque menace se matérialise.
- Évaluation de la gravité: consiste à déterminer l'incidence potentielle de chaque menace.
- Évaluation des menaces: consiste à attribuer à chaque menace des niveaux de menace, basée sur le tableau des niveaux de menaces.

LA PHASE D'ÉVALUATION DES VULNÉRABILITÉS

Cette phase comprend cinq processus :

- Recensement des mesures de protection : consiste à établir une liste de toutes les mesures de protection existantes comprises dans la portée de l'évaluation.
- Évaluation de l'efficacité des mesures de protection: consiste à évaluer l'efficacité des mesures de protection pour réduire les risques éventuels.
- Identification des vulnérabilités: consiste à recenser d'autres vulnérabilités qui exposent les actifs compris dans la portée de l'évaluation.
- Analyse de l'incidence des vulnérabilités: consiste à évaluer les effets des vulnérabilités sur la probabilité de réalisation des menaces, la probabilité de compromission et la gravité des dommages qui en découlent.
- Évaluation des vulnérabilités : consiste à attribuer à chaque vulnérabilité, des niveaux de vulnérabilité, basée sur le tableau des niveaux de menaces.

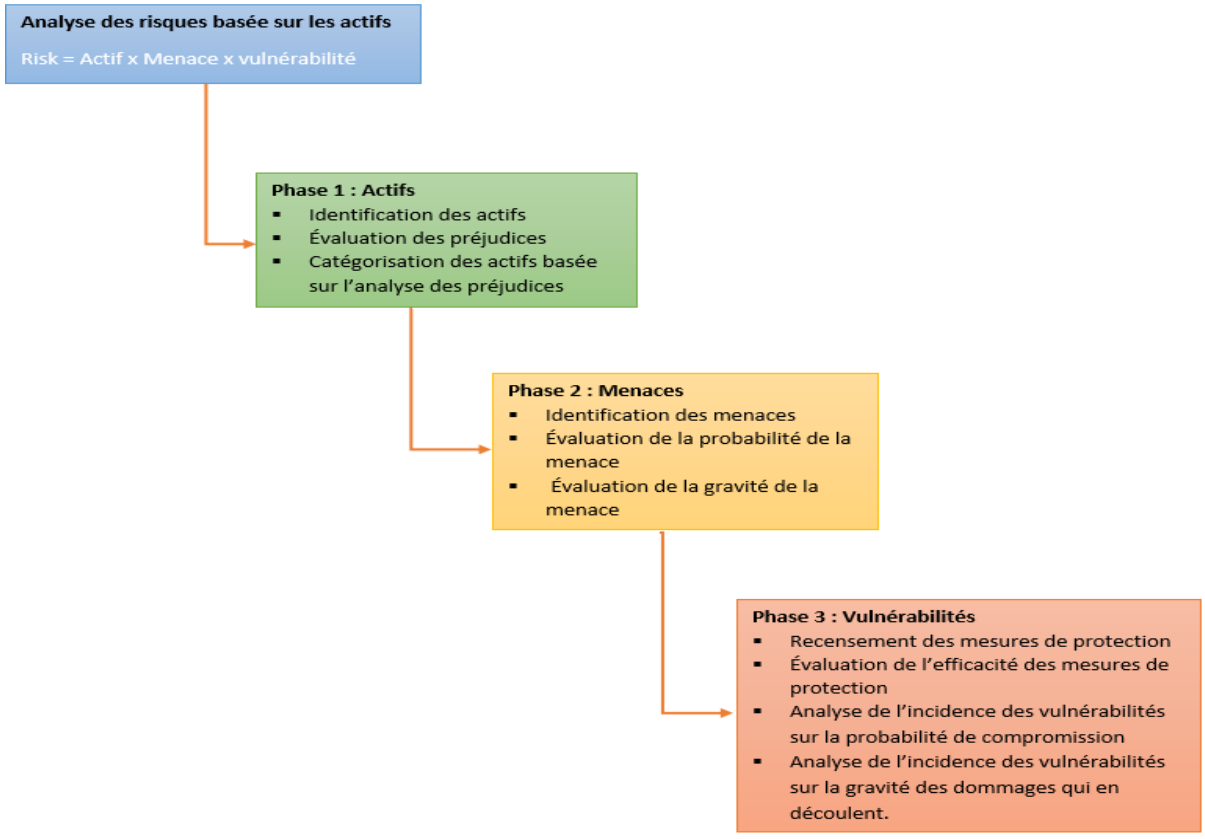

Figure 10 : Analyse des risques basée sur les actifs

RÉVISIONS

Date	Action	Auteur	Version
2022-10-08	Version précédente	CESI de l'UQ	1.0
2022-10-24	▪ Ajout des titres pour chaque figure ▪ Figure pour montrer la différence entre une analyse de préjudice et analyse de risque ▪ Ajout de la notion de risque dans la section qu'est-ce que la catégorisation des actifs informationnels ▪ Ajout de quelques exemples de normes de conformité	CESI de l'UQ	1.1
2024-02-28	▪ Changement du TLP à diffusion permise	CESI de l'UQ	1.2

GLOSSAIRE

- **Pilote du système évalué** : toute personne clé ayant une bonne connaissance de ses processus d'affaires, leurs interrelations et les services offerts aux établissements de l'Université de Québec qui sont spécifiques au système évalué.
- **Atteinte à la vie privée :** elle se caractérise par la collecte, l'usage, la communication, la conservation ou le retrait inapproprié ou non autorisé de renseignements personnels. Ces activités sont considérées "incorrectes" et "non-autorisées" lorsqu'elles contreviennent aux lois applicables en matière de protection des renseignements personnels.
- **Inconfort physique :** Il s'agit d'une situation d'inconfort qui cause une gêne physique ou morale à un citoyen.
- **Douleur physique, blessure, traumatisme, difficultés, maladie :** C'est un préjudice qui peut occasionner de la douleur physique, blessure, du traumatisme ou d'autres difficultés à un citoyen.
- **Stress :** Le stress est une réaction humaine normale qui arrive à tout le monde. En fait, le corps humain est conçu pour subir un stress et y réagir. Lorsque vous subissez des changements ou des défis (facteurs de stress), votre corps produit des réponses physiques et mentales. C'est le stress.
- **Qualité de vie affectée** : La perception qu'a un individu de sa place dans l'existence, dans le contexte du système de valeurs dans lequel il vit, en relation avec ses objectifs, ses attentes, ses normes et ses inquiétudes. Par exemple, un citoyen doit rembourser une dette contractée à son nom et à son insu par un individu malveillant (vol d'identité) ou payer pour des services qu'il n'a pas consommés.
- **Perte de confiance** : C'est une inquiétude ou un questionnement partagé par rapport à un incident de sécurité.
- **Perte financière engendrant un stress ou un inconfort** : il y a perte financière lorsque le client ou l'organisation, selon des circonstances perd de l'argent ou reçoit des montants inférieurs à ce qui avait été initialement prévu. Il s'agit notamment du ressenti relatif à une situation où l'individu doit prendre en charge tout ou en partie des dépenses avant de recevoir le montant dû (paie, compte à recevoir, etc.).
- **Objet de catégorisation** : Un objet de catégorisation peut être assimilé à un processus, un regroupement d'actifs informationnels ou un actif informationnel. C'est l'élément auquel on attribue les niveaux d'impact sur le plan de la DIC.