Technopédagogie

ANALYSE DES BESOINS

Par : Daniel Joseph / Marie Sarone Kolfir / Rachelle Pelletier

Le 7 décembre 2021

TABLE DES MATIÈRES

1. LE MANDAT

1.1 Informations sur le client

Le client, une organisation gouvernementale qui gère des informations sensibles et stratégiques au Québec. Il a pour mission d'assurer une veille, sur le plan stratégique, des enjeux de sécurité ainsi que des menaces susceptibles de porter atteinte à la sécurité de l'information gouvernementale (Secrétariat du Conseil du trésor, 2014, p. 17).

À l'interne, cette organisation est confrontée à un enjeu de gestion de la sécurité de l'information par les gestionnaires détenteurs de l'information. En effet, ces derniers sont responsables des systèmes informatiques contenant des informations confidentielles et sensibles, et de leur sécurité.

1.2 Contexte du projet

Dans toute organisation, l'information est un patrimoine économique qui doit être protégé et sécurisé (Dominique, D. de P., 2013, p. 19). Dans cette organisation, ce besoin est tout à fait présent, car le foisonnement de nouvelles technologies procure certes de nombreux et importants avantages et des occasions à saisir, mais il s'accompagne cependant de nouveaux risques qu'il faut gérer avec beaucoup d'attention (Fondation canadienne pour l'audit et la responsabilisation, 2018, p. 5). Les virus informatiques, les rançongiciels, l'hameçonnage, le piratage informatique et l'usurpation ou le vol d'identité sont les risques les plus connus.

Face à l'exposition constante à ces risques, l'organisation s'est engagée à mettre en place des mesures essentielles pour assurer la protection de l'information contre toute tentative non autorisée d'accès, d'utilisation, de modification ou de destruction (s.n., 2021, paragr. 1). L'une de ces mesures est de se conformer au cadre gouvernemental provincial en matière de sécurité publique en confiant la responsabilité de la sécurité des informations de cette organisation aux gestionnaires détenteurs de l'information.

2. BESOIN D'AFFAIRES

2.1 Besoin de se conformer

Le besoin d'affaires est de se conformer au cadre gouvernemental provincial en matière de sécurité publique afin d'améliorer la gestion de la sécurité de l'information détenue par 60 gestionnaires détenteurs de l'information.

Une analyse des besoins est effectuée dans le présent document pour répondre aux besoins d'affaires de l'organisation. Les résultats de cette analyse permettent de comprendre les motifs de l'insuffisance des solutions antérieures, d'identifier les besoins réels des détenteurs de l'information et de proposer des actions adéquates pour renforcer les efforts déjà déployés.

2.2 Efforts déployés

De 2016 à 2021, l'organisation a mis en œuvre un programme de sensibilisation obligatoire pour tous les employés sur l'importance d'adopter de bonnes pratiques en matière de sécurité de l'information (s.n, intranet, paragr.1).

Selon le Rapport annuel de gestion 2020-2021, la Direction générale des services à la gestion offre ses services de soutien et de conseil à l'ensemble des unités de cette organisation, dont la direction qui s'occupe de la sécurité des technologies et des systèmes d'information (s.n, 2021, p. 16).

Pendant la pandémie, l'organisation a eu à relever des défis internes dont un déploiement d'outils numériques et une amélioration de la mobilité du personnel visant à répondre aux nouveaux besoins créés par les circonstances, notamment par la distribution d'ordinateurs portables, l'installation du logiciel Teams et le rehaussement de la sécurité et du réseau pour l'accès à distance (s.n, 2021, p. 14).

Cette transformation fut accompagnée de la diffusion de documents et de capsules d'informations via l'intranet ainsi qu'une politique portant sur la sécurité de l'information (PSI) et comportant une description des rôles et responsabilités des détenteurs de l'information (s.n, 2021).

2.3 Insuffisance des moyens mis en place

Les moyens mis en place n'étaient pas centrés sur les besoins des détenteurs. Donc, en dépit de ces efforts, la performance des détenteurs est encore problématique au sein de cette organisation, vu qu'ils ont des réactions différentes, voire tardives, face à un incident de sécurité. De plus, ils ont tendance à se déresponsabiliser au lieu d'assumer adéquatement leurs rôles et responsabilités en gestion de la sécurité de l'information puisqu'ils estiment que la gestion de la sécurité de l'information relève de la Direction des technologies de l'information. Le comportement des détenteurs d'information laisse comprendre qu'ils ne sont pas pleinement conscients de leur imputabilité et qu'ils n'ont pas tous le même niveau d'information quant à leurs rôles et responsabilités.

Dans ce contexte, l'organisation a décidé d'agir en amont en s'engageant dans une démarche d'identification et de résolution de problèmes. Cet exercice est validé par le client qui a accepté de participer au processus en signant un formulaire de consentement (annexe I).

3. MÉTHODOLOGIE DE COLLECTE

La stratégie de collecte d'informations, incluant les questions, est basée sur le modèle de Chevalier, (2002, p. 12) puisque la grille d'analyse de la performance (annexe V) permet de dégager une meilleure vue d'ensemble de l'état de la situation en chiffrant les éléments positifs et négatifs au sein de cette organisation. En effet, cette grille d'analyse permet de comprendre les niveaux de performance actuels et désirés, et d'établir des objectifs raisonnables liés aux facteurs de performance.

3.1 Analyse documentaire

L'organisation dispose d'un intranet dans lequel on retrouve certaines informations telles que la Politique ministérielle de sécurité de l'information ; le Programme de sensibilisation à la sécurité de l'information, ainsi que plusieurs procédures, directives, politiques, charte, formulaire et guide. Certains de ces documents (annexe VI) ont été consultés.

3.2 Entrevues

Deux entrevues (annexe II et III) d'une durée d'une heure pour la première et d'une heure trente, pour la seconde, ont été faites auprès de deux gestionnaires de cette organisation. Une dizaine de questions semi-ouvertes comportant plusieurs sous-questions leur ont été posées afin de bien comprendre les problématiques de gestion de la sécurité vécues au sein de l'organisation.

3.3 Questionnaire en ligne

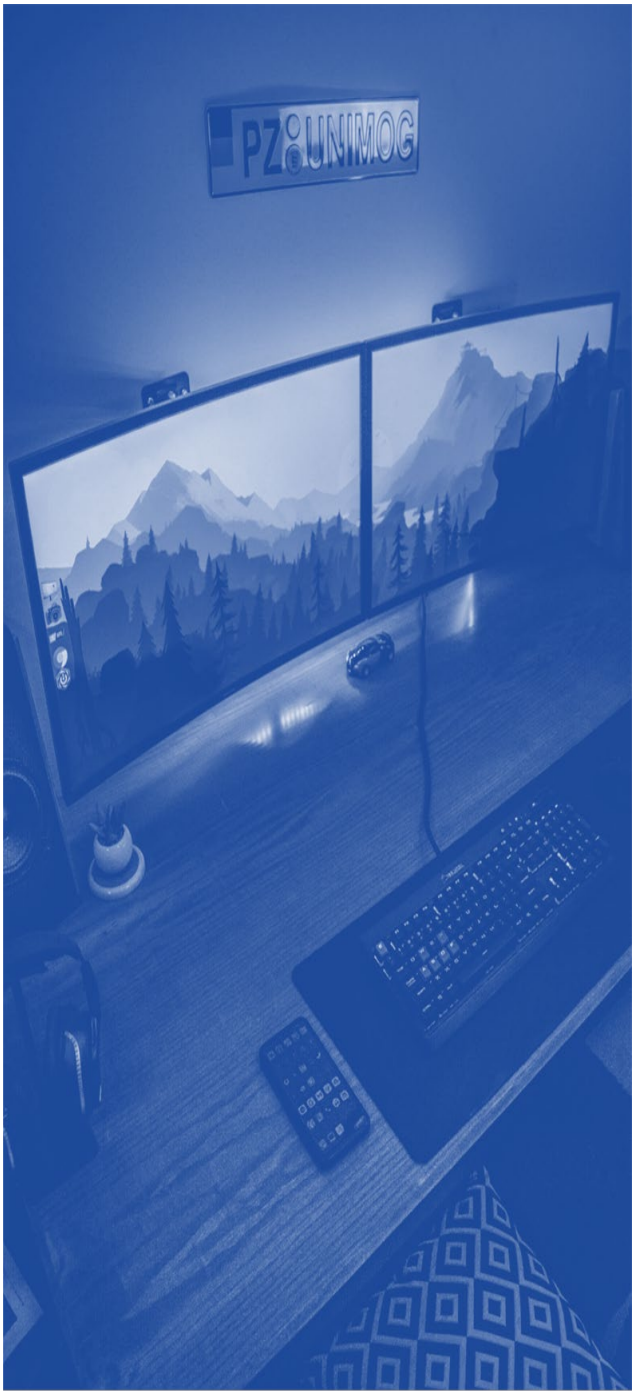
Un questionnaire (annexe IV) en ligne destiné aux apprenants potentiels et comportant plusieurs questions semi-ouvertes a été aussi conçu afin d'obtenir des données probantes sur ces derniers.

3.4 Limitations

Nous avons eu accès à seulement un apprenant, par manque de disponibilité et de temps. Sinon, un bassin de 60 détenteurs aurait pu répondre aux questions portant sur leurs besoins réels pour améliorer leurs performances.

4. PORTRAIT DES APPRENANTS

Le groupe d'apprenants est composé d'environ 60 gestionnaires détenteurs qui travaillent dans plusieurs directions et secteurs d'activités de l'organisation. Ils ont tous accès à des ordinateurs et d'autres outils technologiques, mais leurs habiletés en gestion de la sécurité de l'information diffèrent beaucoup. De plus, ils ont des expériences et des expertises variées comme détenteurs.

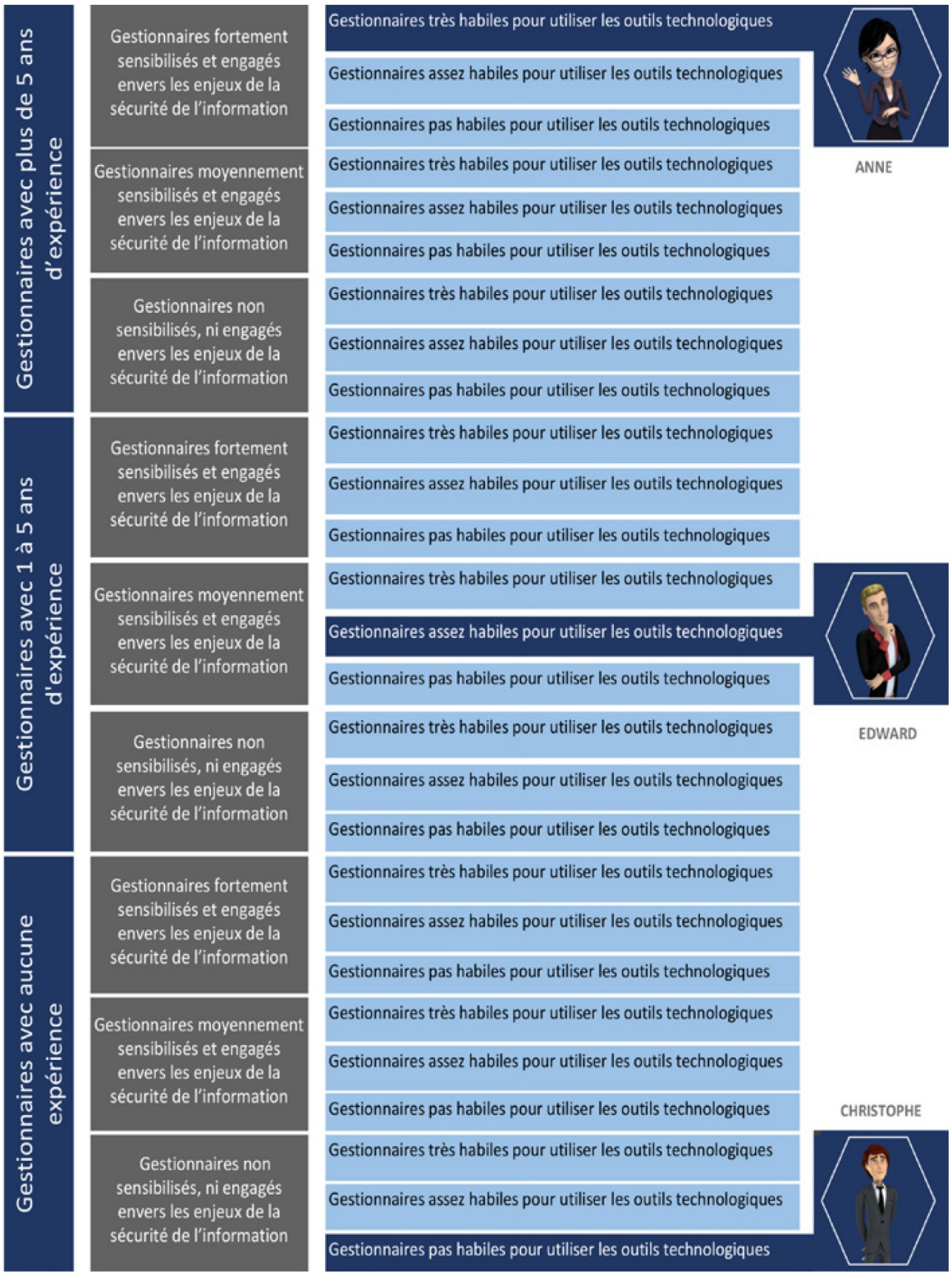


Trois des facteurs influençant leur apprentissage se définissent comme suit :

- Leur niveau d'expérience à titre de gestionnaires détenteurs d'informations;
- Leur niveau de sensibilisation et d'engagement quant aux enjeux de sécurité de l'information;
- Leur habilité à utiliser les outils technologiques.

Le tableau suivant présente trois personas comportant trois positionnements par rapport aux caractéristiques.

4. Portrait des apprenants



4.1 Description des personas

Anne Robitaille

Âgée de 61 ans, Anne est directrice des technologies de l'information.

Elle est gestionnaire depuis plus de 15 ans et détentrice d'informations depuis plus de 10 ans. Ayant déjà occupé un poste de gestionnaire des incidents informatiques, elle est fortement sensibilisée et engagée aux enjeux de sécurité de l'information.

La sécurité de l'information étant l'une de ses priorités, elle est très disponible pour suivre les formations requises pour exercer ses fonctions.

Edward Ficher

Âgé de 55 ans, Edward possède quatre années d'expérience en gestion, incluant de l'expérience comme détenteur.

Il est moyennement sensibilisé et engagé aux enjeux de sécurité de l'information. Il a suivi des capsules vidéo de sensibilisation en sécurité au même titre que d'autres employés, sans plus.

Il demeure régulièrement disponible pour effectuer des formations en ligne.

Christophe Irdehen

Christophe est gestionnaire depuis 6 mois. C'est sa première expérience comme gestionnaire et comme détenteur. Il n'est aucunement sensibilisé ni engagé aux enjeux de sécurité de l'information. Comment cela se manifeste-t-il ?

Il a beaucoup de difficulté à gérer son emploi du temps, ce qui a pour conséquence qu'il n'est jamais disponible pour suivre des formations en ligne.

4.2 Portrait de la situation actuelle et de la situation idéale

Les mises en situation suivantes permettent de visualiser l'écart des performances actuelles par rapport au niveau des performances désirées dans le comportement d'un gestionnaire détenteur.

SITUATION ACTUELLE

Un lundi matin, Mme Giselle, directrice des ressources humaines depuis 2 ans et détentrice du système (Xpdotation) commence sa journée en se connectant à Xpdotation à l'aide d'un mot de passe collé sur son ordinateur. Quelques minutes plus tard, un employé lui demande de l'aide afin de définir le niveau de sensibilité d'un document dans Xpdotation. Elle attribue une mauvaise étiquette au document, qu'elle classe comme public alors que c'est hautement confidentiel. Les informations sont dorénavant visibles par l'ensemble des utilisateurs d'Xpdotation.

Au cours de la journée, elle imprime une liste complète des informations sensibles, sans la récupérer à l'imprimante. Cette même liste, imprimée à la fin des cinq dernières semaines, est laissée sur son bureau à la vue de tout le monde. La journée avance et elle se rappelle que cela fait plusieurs jours qu'elle ne retrouve pas la clé USB contenant une copie des informations d'Xpdotation qu'elle avait fait pour lui permettre de faire du télétravail. Après une recherche auprès des employés, sans succès, elle fait un appel au support informatique pour les informer de la situation. Lors de son appel, elle mentionne qu'au final, cela fait environ trois semaines qu'elle ne sait pas où se trouve cette clé USB. Elle décrit les informations qui s'y trouvaient et elle précise que la clé USB était protégée d'un mot de passe connu de tous les employés, car c'est le même mot de passe qui est utilisé pour toutes les clés USB de la direction.

La journée tire à sa fin et elle quitte son bureau en laissant son poste de travail déverrouillé et les portes de son bureau ouvertes. Près de la sortie, elle retrouve une page comportant des informations confidentielles provenant du système Xpdotation. Elle écrase le document et le jette dans la poubelle (pour documents non confidentiels) avant de partir pour la maison.

SITUATION IDÉALE

En commençant sa journée, Mme Giselle, directrice des ressources humaines depuis 2 ans et détentrice du système (Xpdotation) utilise un mot de passe multifactoriel pour se connecter au système Xpdotation. Elle y effectue les tâches qui lui sont assignées comme détentrice et se déconnecte du système avant de procéder à ses autres tâches (courriel, appel, etc.). Au cours de la journée, elle fait une rencontre avec un chef d'équipe de son secteur, pour gérer les données sensibles. Parmi les documents reçus dans sa direction, elle vérifie la nécessité de collecter ces informations et procède au suivi, à la catégorisation et à l'étiquetage des données sensibles. Elle procède tout de suite après à une vérification des gens qui ont demandé un accès aux informations dans Xpdotation et demande des clarifications pour les cas suspects.

Plus tard dans la journée, le chef d'équipe lui mentionne un cas probable de fuite d'informations. Elle déclare immédiatement le cas suspect à l'équipe de gestion des incidents pour investigation. Au cours de cette même journée, à deux reprises, après des vérifications, elle recadre des employés pour des erreurs dans le traitement des données sensibles. Elle prend le temps de discuter, d'expliquer les processus mis en place et recommande les bonnes pratiques à ses employés, comme elle le fait régulièrement aussi avec ses autres collègues gestionnaires. Elle organise régulièrement des rencontres d'équipe et la sensibilisation des employés en sécurité de l'information est un sujet à l'ordre du jour, une fois par mois. Elle leur propose des activités de sensibilisation et des formations ciblées portant sur la cybersécurité.

En fin de journée, elle fait un appel auprès du directeur de l'équipe des technologies de l'information afin de vérifier que les travaux avancent quant à l'installation des logiciels nécessaires pour bien protéger les données sensibles du système Xpdotation. En quittant son bureau, elle vérifie qu'il n'y a pas de documents traînant sur son bureau et que toutes les informations sensibles sont placées dans un classeur fermé à clé ou dans Xpdotation.

5. FONCTIONS ET OBJECTIFS

5.1 Besoins fonctionnels

Les besoins fonctionnels suivants sont identifiés dans le cadre de la performance idéale à atteindre par les détenteurs:

1. Définir les rôles de chacun au sein de cette organisation

    1.1 Se référer à la Direction des technologies de l'information.
    1.2 Distinguer les rôles et responsabilités des gestionnaires détenteurs.
    1.3 Identifier un actif informationnel.

2. Gérer l'information selon son cycle de vie.

    2.1 Catégoriser l'information selon sa disponibilité, son intégrité et son niveau de confidentialité.
    2.2 Tester la nécessité de l'utilisation des données sensibles.
    2.3 Étiqueter les données sensibles selon leur niveau de sensibilité.

3. Vérifier que les mesures de sécurité de l'information mises en place sont adéquates.

    3.1 Utiliser un mot de passe multifactoriel pour chaque actif.
    3.2 Vérifier en continu les accès aux systèmes d'information.
    3.3 Vérifier l'avancement des travaux de mise à jour et à niveau les différents systèmes.

4. Vérifier que les mesures de sécurité de l'information sont suivies par les employés de cette organisation.

    4.1 Expliquer aux employés les directives de protection des informations sensibles.
    4.2 Déclarer tout incident de sécurité à l'équipe informatique.
    4.3 Recadrer des employés pour des erreurs dans le traitement des données sensibles

5.2 Objectif d'affaires

Le besoin d'affaires est de se conformer au cadre gouvernemental provincial en matière de sécurité publique afin d'améliorer la gestion de la sécurité de l'information détenue par 60 gestionnaires détenteurs de l'information. Pour y arriver, la participation de plus de 75 % des détenteurs en poste pour chaque année financière est requise.

5.3 Objectifs d'apprentissage

L'organisation vise à renforcer les compétences des gestionnaires détenteurs de l'information en gestion de sécurité de l'information, en conformité avec la Politique ministérielle de sécurité de l'information (PSI). Donc, à la fin de l'intervention :

OBJECTIF 1

1. Étant donné les responsabilités en gestion de la sécurité de l'information identifiées par l'organisation gouvernementale, définir adéquatement[1] son rôle au sein de cette organisation en matière de sécurité de l'information.

    1.1 Étant donné l'obligation de divulguer tout incident de sécurité de l'information, se référer immédiatement à la Direction des technologies de l'information pour toute question ou tout incident.

    1.2 Étant donné l'imputabilité du détenteur comme décrite dans la PSI, distinguer l'ensemble de ses rôles et responsabilités par rapport à ceux des autres gestionnaires.

    1.3 Étant donné l'obligation de prévenir les risques liés à la protection des informations de chaque actif, identifier tous les actifs informationnels sous sa gouverne.

OBJECTIF 2

2. Étant donné le volume de données sensibles reçues, gérer systématiquement et de façon satisfaisante[2] toute l'information tout au long de son cycle de vie.

    2.1 Étant donné les risques de fuite des données sensibles, tester[3] la nécessité de leur utilisation dans 100 % des cas.

---

[1] Selon les rôles et responsabilités décrits dans la PSI.

[2] « De façon satisfaisante » signifie au respect des critères décrits dans la PSI.

[3] Tester la nécessité est le jargon utilisé par le client pour désigner le terme « vérifier » que les critères d'utilisation des données sensibles sont vraiment nécessaires.

2.2 Compte tenu de l'ampleur des données à gérer, bien catégoriser toutes les informations selon leur disponibilité, leur intégrité et leur niveau de confidentialité attribué, selon le cas.
2.3 Étant donné l'obligation d'identifier et de suivre les données sensibles, étiqueter immédiatement, 100 % des informations selon leur niveau de sensibilité.

OBJECTIF 3

3. Étant donné les menaces de sécurité de l'information auxquelles est constamment exposée l'organisation, vérifier que toutes les mesures de sécurité sont mises en place adéquatement[4].

3.1 Étant donné la nécessité de contrer des incidents de sécurité, utiliser, pour chaque actif, un mot de passe multifactoriel pour 100 % des connexions.
3.2 Étant donné un haut taux de roulement de personnel, compléter une vérification mensuelle des accès octroyés pour chaque système d'information.
3.3 Compte tenu de l'évolution constante des risques, vérifier mensuellement l'avancement des travaux de mise à jour et à niveau des différents systèmes.

OBJECTIF 4

4. Étant donné l'obligation de maintenir la confidentialité des données, vérifier régulièrement que les mesures de sécurité de l'information sont respectées par les employés.

4.1 Étant donné les risques de sécurité de l'information pour chaque accès octroyé, expliquer systématiquement aux employés les directives de protection des informations sensibles.
4.2 Étant donné l'obligation d'une prise en charge rapide des incidents de sécurité, déclarer immédiatement 100 % des cas suspects et incidents de sécurité à l'équipe informatique.
4.3 Étant donné les risques liés à la manipulation des informations sensibles, recadrer les employés pour chaque erreur dans le traitement des données sensibles.

[4] Selon les standards définis dans la PSI.

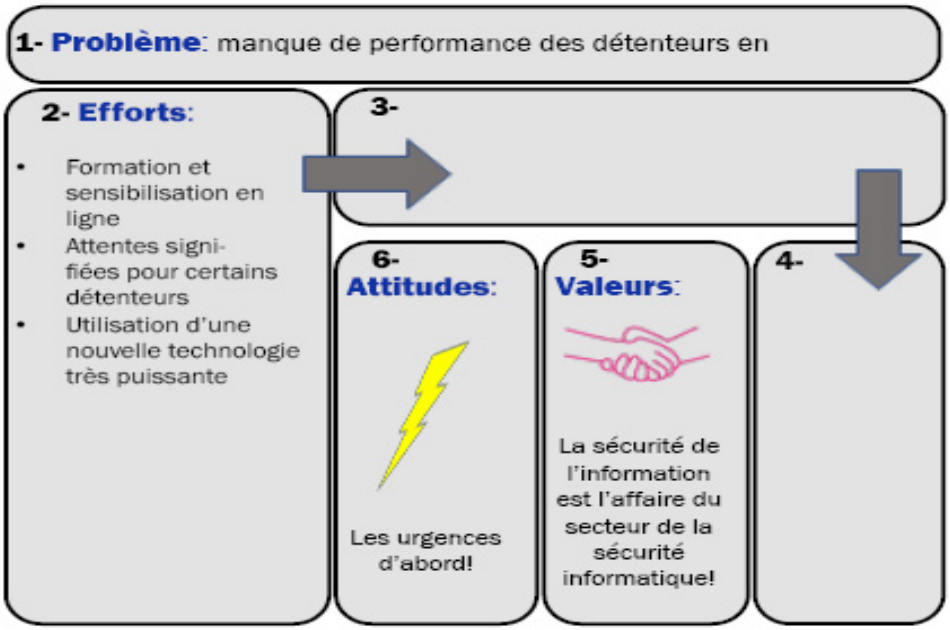
6. ANALYSE DES CAUSES PROFONDES

6.1 Étapes de la représentation Paradoxe

L'approche retenue pour l'analyse des causes profondes est basée sur l'adaptation du modèle de Chevalier (2002, p. 12) et de représentation Paradoxe (Chevalier, Buckles, et Bourassa, 2013, p.71-72). Étant limités dans le temps, quelques résultats positifs et négatifs de la grille d'analyse de Chevalier ainsi que les étapes 2, 5 et 6 de la représentation Paradoxe guident cette démarche.

Les étapes 2, 5 et 6 de Paradoxe (figure 1) utilisées dans cette analyse contribuent à déterminer les causes profondes du manque de performance des détenteurs au sein de cette organisation. Ainsi, la deuxième étape consiste à présenter les efforts déployés pour résoudre le problème, la cinquième et la sixième révèlent des éléments dans l'organisation comme les valeurs et les attitudes qui contribuent à maintenir le problème. À ces étapes, s'ajoute l'influence de l'environnement de travail sur la performance des apprenants.

Figure 1- Modèle Paradoxe



6.1.1 Efforts déployés au sein de l'organisation (étape 2)

La haute direction fait de la sécurité de l'information une priorité. Comme mentionné dans la description du mandat, plusieurs efforts sont déployés pour la gestion de la sécurité de l'information. Des capsules de sensibilisation ou de formation sont diffusées sur l'intranet de cette organisation pour sensibiliser le personnel sur la sécurité de l'information, mais elles ne comportent pas des informations spécifiques aux détenteurs.

Les deux répondants aux entrevues rapportent que la gestion de la sécurité de l'information fait partie des leurs attentes signifiées en début d'année. Compte tenu de leur rôle au sein de l'organisation, ils se sentent imputables par différents mandats qui leur sont donnés pour rehausser la sécurité de l'information, contrairement aux autres détenteurs. Ces mandats comportent la gestion des accès, la gestion des incidents, la catégorisation des informations dans le système. Ils révèlent aussi que l'organisation dispose d'une technologie très puissante depuis moins d'un an avec le soutien ministériel et gouvernemental. Les analyses font état de recrutement des gestionnaires compétents. Le contexte et l'environnement de travail deviennent nettement plus favorables qu'ils étaient antérieurement.

Malgré tous ces efforts déployés dans l'organisation, d'autres facteurs internes continuent de miner la performance de certains détenteurs.

6.1.2 L'environnement de travail des apprenants (grille d'analyse de Chevalier)

Le niveau de sécurité des infrastructures de développement ainsi que le manque de ressources ont longtemps généré des failles au sein des systèmes. La transformation soutenue en cours depuis le début de la pandémie crée un contexte de travail difficile pour les équipes. Elle ajoute un cran de plus sur la pression de ces équipes. Les apprenants empilent depuis le début de la pandémie des réunions constantes. Le télétravail a pour effet de les rendre plus disponibles dans des plages horaires plus grandes, ce qui devient épuisant pour eux à la longue. Les équipes ont à gérer les surcharges de travail et la contradiction entre les priorités et les urgences.

6.1.3 Valeur adoptée au sein de l'organisation (étape 5)

Les détenteurs externes au secteur de la sécurité de l'information ont une impression selon laquelle cette responsabilité relève de la Direction de la sécurité de l'information (DSI) alors que c'est une responsabilité partagée. Cette impression est considérée comme une valeur organisationnelle et elle influence le comportement des détenteurs qui tardent souvent à informer ou n'informent pas du tout la DSI des incidents survenus dans leur unité. Parfois, ils ne savent pas où et à qui s'adresser et leurs réactions sont différentes. Les analyses effectuées révèlent les absences d'échange d'informations et de climat collaboratif entre les détenteurs sur la sécurité de l'information. Cela contribue à maintenir les problèmes de sécurité de l'information.

6.1.4 Attitudes des détenteurs de l'information (étapes 6)

En termes d'attitudes, les détenteurs se conforment aux pratiques courantes de gestion des tâches dans L'organisation pour se conformer aux valeurs de l'organisation vu qu'ils ont une connaissance limitée de leurs rôles et responsabilités. Leurs motivations sont bien alignées avec le travail à réaliser, mais les attentes de l'organisation ne sont pas clairement définies. Travaillant sur des dossiers de transformation, ils doivent souvent conjuguer avec des interdépendances entre différentes priorités, ce qui peut générer des conflits et amener leurs équipes à reprendre du travail pour corriger des éléments à cause d'incompatibilités. Ils sont souvent appelés à mettre sur pause leur travail affecté à des priorités pour répondre à des urgences. Cela retarde l'accomplissement des priorités dont les échéances ne changent pas et accroît la pression sur les équipes pour les réaliser à temps. Certaines requêtes complexifient leurs tâches.

7. CONTRAINTES

Plusieurs contraintes ont été détectées au sein de l'environnement de travail pouvant affecter le niveau de performance des apprenants.

7.1 Contraintes de temps et d'espace

Les apprenants sont isolés physiquement puisqu'ils se retrouvent dans différents types d'établissements (services de police et de prévention de la criminalité, de sécurité civile, de sécurité incendie, des services correctionnels et de sciences judiciaires et de médecine légale) et ils sont dispersés dans plusieurs régions administratives du Québec.

Compte tenu des différents types d'établissements sous la charge de cette organisation, les différents environnements de travail sont sécurisés au niveau de la sécurité physique (accès restreint) afin de protéger au maximum les employés. En effet, à la suite d'un audit de sécurité physique, des correctifs ont été apportés pour corriger la situation (système de cléage).

Compte tenu de la multitude de responsabilités des gestionnaires, la solution retenue doit être adaptée à leur contexte de gestion (rôle officiellement expliqué) et de gestion des situations d'urgences.

7.2 Contraintes budgétaires

Il y a des contraintes budgétaires pour l'élaboration de la solution retenue pour le client, mais le montant alloué pour le projet sera défini en fonction des solutions proposées et retenues.

7.3 Contraintes technologiques

L'environnement numérique s'est beaucoup modernisé, mais il ne l'est pas complètement. En allant vers l'infonuagique, L'organisation doit déployer et sécuriser divers systèmes informatiques modernes. L'ensemble des nouveaux systèmes informatiques n'existe pas encore. En outre, les solutions retenues doivent prioriser l'utilisation des technologies récemment déployées afin de maximiser le retour sur investissement de cette organisation.

8. LES ÉVALUATIONS

8.1 Évaluation des apprenants

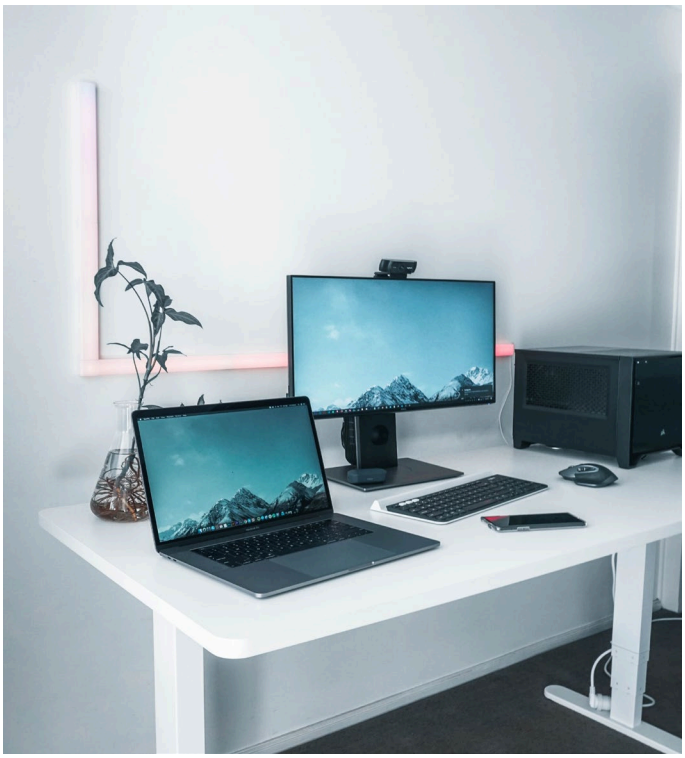
Pour mener l'évaluation sommative des apprenants dans la situation idéale de gestion de la sécurité de l'information après leur formation, les trois outils suivants sont proposés.

8.1.1 La mise en situation

Deux mois après l'activité, un exercice de mise en situation est prévu dans le but de déterminer le niveau de connaissances des rôles et responsabilités que les apprenants ont acquis en matière de sécurité de l'information à la suite de la solution retenue. Des scénarios (par exemple, situation actuelle de Mme Giselle, à la page 10) permettant aux apprenants de vivre différents types d'incidents seront élaborés afin de pouvoir évaluer, à l'aide d'une grille d'évaluation, leurs comportements à titre de détenteurs. Une analyse de leur comportement mettra en lumière le niveau de connaissances assimilées dans le cadre de l'intervention sur la gestion de la sécurité de l'information.

8.1.2 Observation en deux étapes

Une première étape d'observation sera réalisée au sein de l'organisation en vue d'évaluer les connaissances des détenteurs à la suite de l'activité choisie. Une deuxième étape d'observation participative sera réalisée (durant les 6 mois suivant le déploiement de l'activité) au sein de l'organisation en vue de déterminer le niveau d'application des connaissances acquises par les apprenants en matière de gestion de la sécurité de l'information. Une collègue travaillant dans cette organisation se chargera d'observer les comportements des détenteurs et leur attribuer des scores à chaque réaction dans une situation donnée. L'outil de collecte de données utilisé sera la grille d'observation (un exemple est proposé à l'annexe VII). Elle comporte différents énoncés relatifs à la gestion de sécurité de l'information. Chaque réaction des détenteurs sera évaluée dans cette dernière.



8.1.3 Questionnaire auprès des gestionnaires détenteurs

Le questionnaire en ligne (annexe IV) utilisé dans la collecte de données pour l'analyse de besoins sera transmis aux nouveaux gestionnaires détenteurs, 7 mois après leur nomination et leur participation à l'activité, afin d'évaluer leur niveau de connaissances quant à leurs rôles et responsabilités. Avec la mise en place d'une nouvelle structure qui transmet une lettre de la haute direction aux nouveaux gestionnaires détenteurs de l'information sur leurs rôles et responsabilité et leur imputabilité, nous voulons nous assurer que cette nouvelle procédure se révèle pertinente et efficace.

8.2 Lien entre l'évaluation sommative et l'objectif d'affaires

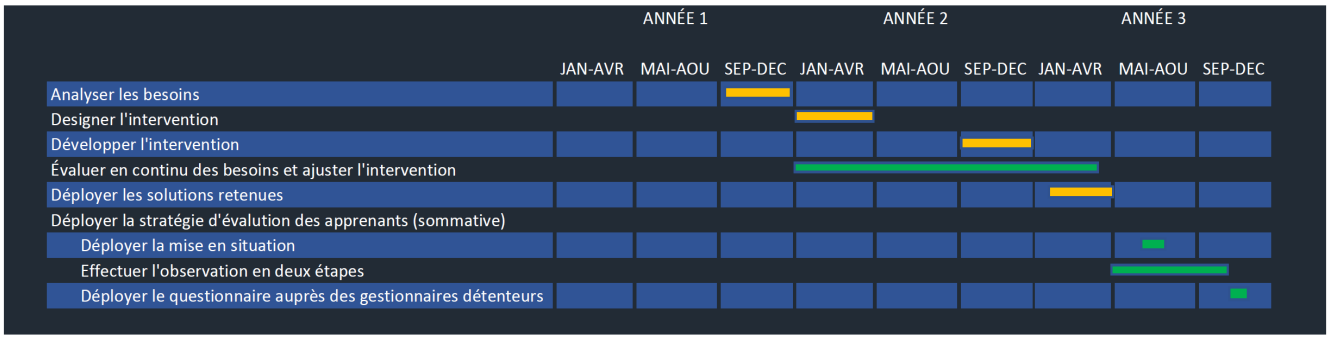
L'évaluation sommative permet aussi de faire le lien entre les résultats de l'intervention retenue et l'objectif d'affaires du projet. Étant donné le désir de cette organisation de se conformer à la PSI et d'effectuer un contrôle des coûts quant au nombre d'incidents, nous prévoyons évaluer le résultat à la suite de la solution proposée. En plus des mises en situation, des observations et du questionnaire en ligne, la compilation des données collectées permettra un suivi en continu du nombre d'apprenants invités à participer à l'activité. L'objectif est de s'assurer d'avoir une participation de plus de 75 % des détenteurs en poste pour chaque année financière.

8.3 Échéancier

Comme le démontre la figure 2, l'évaluation sommative de l'intervention à l'aide de la mise en situation, de l'observation ainsi que du questionnaire est prévue durant les 7 mois suivant le déploiement de l'intervention. Afin d'intervenir le plus tôt possible après l'intervention, une mise en situation est prévue deux mois suivant l'activité. Cette étape permettra d'identifier les connaissances acquises et de rectifier les comportements non désirés par l'organisation.

Les deux étapes d'observation se dérouleront durant les 6 mois suivants l'intervention. Cette durée est proposée, afin de vérifier dans le temps, à quel niveau les apprenants appliquent ce qu'ils ont appris pendant l'intervention. De plus, un questionnaire destiné aux gestionnaires détenteurs est proposé 7 mois après l'activité afin de compléter le processus d'évaluation de chaque apprenant.

Figure 2 - Calendrier des évaluations



9. ANNEXES

I. Formulaire de consentement

Titre du projet : Analyse des besoins et solutions existantes en formation sécurité de l'information pour les détenteurs

Présentation de l'équipe

Ce projet est réalisé dans le cadre d'un travail d'équipe effectué par Rachelle Pelletier, Daniel Joseph et Marie Sarone Kolfir dans le cadre du cours Approche systémique et analyse de besoins (TEN-7001), du département d'études sur l'enseignement et l'apprentissage de la Faculté des sciences de l'éducation à l'Université Laval.

Avant d'accepter de participer comme répondants aux entrevues dans le cade de ce projet, veuillez prendre le temps de lire et de comprendre les renseignements qui suivent. Ce document vous explique le but de ce projet, ses procédures, avantages, risques et inconvénients. Nous vous invitons à poser toutes les questions que vous jugerez utiles à la personne qui vous présente ce document.

Nature du projet

Ce projet consiste à recueillir les informations nécessaires sur la formation des détenteurs en gestion de la sécurité de l'information. Le but est de procéder à une analyse systémique et rigoureuse des besoins du ministère en lien avec la performance des détenteurs avant de proposer des solutions pour mieux répondre aux besoins de performance des apprenants.

Déroulement de la participation

Votre participation à cette recherche consiste à participer à une entrevue (environ 1 heure, virtuelle) qui portera sur les éléments suivants :

- élément d'information sur les apprenants;
- élément d'information sur la situation actuelle par rapport à la situation idéale;
- élément d'information sur les problèmes et lacunes actuels de performances et portrait d'une situation idéale après l'intervention (Ex. : formation des détenteurs);
- élément d'information sur les objectifs à haut niveau de l'entreprise qui justifie la valeur d'entreprendre ce projet de formation.

Avantages, risques ou inconvénients possibles liés à votre participation

Le fait de participer à ce projet vous offre une occasion de partager votre expérience, de réfléchir et de discuter en toute confidentialité, sur des besoins de formation en sécurité de l'information et des solutions qui pourront être bénéfiques pour votre milieu de travail

Il est possible que le fait de raconter votre expérience suscite des réflexions ou des souvenirs parfois émouvants ou désagréables. Si cela se produit, n'hésitez pas à en parler avec la personne qui mène l'entrevue.

Participation volontaire et droit de retrait

Vous êtes libre de participer à ce projet. Vous pouvez aussi mettre fin à votre participation sans conséquence négative ou préjudice et sans avoir à justifier votre décision. Si vous décidez de mettre fin à votre participation, il est important d'en prévenir Marie Sarone Kolfir. Tous les renseignements personnels vous concernant seront alors détruits.

Confidentialité et gestion des données

Les membres de l'équipe vous assurent la confidentialité sur l'ensemble des informations qui seront collectées dans le cadre de ce projet. À cet égard, voici les mesures qui seront appliquées :

- les noms des participants ne paraîtront dans aucun rapport;
- les divers documents de la recherche seront anonymisés;
- les résultats individuels des participants ne seront jamais communiqués;
- les matériaux de la recherche, incluant les données et les enregistrements, seront conservés sur ordinateur protégés par un mot de passe durant le projet. Ils seront détruits à la fin de la session universitaire, soit en décembre 2021 ;
- les outils et résultats pourront faire l'objet de publications sur des sites ou revues professionnelles, et aucun participant ni le ministère de la Sécurité publique ne pourra y être identifié.

Remerciements

Votre collaboration est précieuse pour nous permettre de réaliser ce projet et nous vous remercions d'y participer.

Signatures

Je soussigné(e)_____consens librement à participer à ce projet intitulé : « Analyse des besoins et solutions existantes en formation sécurité de l'information pour les détenteurs . J'ai pris connaissance du formulaire et j'ai compris le but, la nature, les avantages, les risques et les inconvénients du projet de recherche. Je suis satisfait(e) des explications, précisions et réponses qu'un des membres de l'équipe m'a fournies, le cas échéant, quant à ma participation à ce projet.

_____ _____

Signature du participant, de la participante Date

L'adresse (électronique ou postale) à laquelle je souhaite recevoir une copie du Rapport d'analyse est la suivante : _____

J'ai expliqué le but, la nature, les avantages, les risques et les inconvénients du projet de recherche au participant. J'ai répondu au meilleur de ma connaissance aux questions posées et j'ai vérifié la compréhension du participant.

_____ _____

Signature des membres de l'équipe Date

_____ _____

Signature des membres de l'équipe Date

_____ _____

Signature des membres de l'équipe Date

II. Liste de questions pour le client

1. Vous nous avez formulé un besoin par rapport aux détenteurs de l'information concernant la sécurité d'information. Quel est-il?
    i. Vivez-vous des problèmes de performances au sein des détenteurs en termes de gestion efficace de la sécurité de l'information?
2. La gestion de la sécurité de l'information fait-elle partie des tâches officielles à accomplir par ces gestionnaires?
    i. Est-ce que les détenteurs sont formés pour gérer les incidents de sécurité de l'information?
    ii. Pensez-vous que les détenteurs ont les connaissances requises pour réaliser les tâches associées à la gestion de la sécurité de l'information?
    iii. Pensez-vous que les détenteurs ont les habiletés pour réaliser les tâches requises par la gestion de la sécurité de l'information? (Connaissance/habiletés nécessaires)
3. Existe-t-il des guides pertinents et clairs décrivant les tâches demandées par votre rôle?
4. Que diriez-vous de la performance actuelle des gestionnaires sur le plan de la gestion de la sécurité de l'information. Correspond-elle avec la performance attendue (espérée)?
    i. Comment les détenteurs d'information réagissent-ils lorsqu'il y a des incidents de sécurité de l'information?
    ii. Est-ce que les détenteurs déclarent les incidents de sécurité de l'information?
    iii. Est-ce que les réactions en cas d'incident sont uniformes de la part de tous les détenteurs d'informations?
5. Comment qualifiez-vous votre environnement de travail et ceux des détenteurs de l'information?
    i. Est-ce environnement de travail favorisant une bonne gestion de la sécurité de l'information?
6. Existe-t-il des incitatifs pour encourager les gestionnaires à gérer adéquatement la sécurité de l'information? Incitatifs/financiers ou autres?
7. Comment percevez-vous la motivation des gestionnaires dans la gestion des incidents de sécurité de l'information?
    a. Pouvez-vous lister quelques conséquences de ces incidents de sécurité dans L'organisation?
    b. Avez-vous un moyen de mesurer les conséquences de ces incidents de sécurité de l'information?
8. Échangez -vous entre vous (gestionnaires) sur des enjeux que vous vivez dans la gestion de la sécurité de l'information?
9. Que souhaiteriez-vous améliorer de la part des détenteurs de l'information en gestion de sécurité de l'information au niveau de cette organisation? Info/attentes claires.

III. Liste de questions pour le détenteur

1. Combien d'années d'expérience possédez-vous comme détenteur ?

2. Connaissez-vous l'ensemble de vos rôles et responsabilités à titre de détenteur de l'information?

3. La gestion de la sécurité de l'information fait-elle partie des attentes de cette organisation qui vous ont été clairement signifiées?

4. À titre de détenteur, avez-vous suivi de la formation en gestion de la sécurité de l'information?

5. Un ou des incidents de sécurité de l'information sont-ils déjà survenus au sein de votre équipe?
    a. Quel était le type d'incident ?
    b. Comment avez-vous réagi à ce ou ces incidents? (Advenant qu'un incident se soit produit, comment réagissez-vous?)
    c. Étiez-vous à l'aise à gérer l'incident?
    d. En général, après combien de temps avez-vous réagi à ce ou à ces incidents?
    e. Selon vous, ce ou ces incidents de sécurité de l'information survenus au sein de votre unité étaient-ils évitables? Pourquoi?

6. Quel niveau de priorité accordez-vous à la gestion de la sécurité de l'information parmi l'ensemble de vos tâches quotidiennes de gestionnaires?

7. Selon vous, qu'est-ce qui peut représenter un obstacle à l'accomplissement de vos tâches à titre de détenteur?

8. Qu'est-ce qui pourrait vous motiver à augmenter votre niveau d'implication en gestion de sécurité de l'information, à titre de détenteur?

9. Croyez-vous que les gestionnaires qui sont détenteurs de l'information devraient être imputables dans la gestion de la sécurité de l'information?

10. Avez-vous des suggestions quant aux activités pouvant être mises en place afin d'aider les détenteurs dans leurs rôles à titre de détenteur de l'information?

IV. Questionnaire en ligne destiné aux détenteurs de l'information

Ce questionnaire est disponible en cliquant sur le lien suivant : Lien vers le questionnaire en ligne.

V. Document inspiré de Roger D. Chevalier

Niveau de performance actuel : comportement des détenteurs non conforme à la Politique
Niveau de performance désiré : comportement des détenteurs conforme à la Politique
Objectif raisonnable : acquérir les compétences nécessaires afin de se conformer à la Politique

Facteurs	Stimulations positives (motivations)				Stimulations négatives (démotivations)			
Information	**+4**	**+3**	**+2**	**+1**	**-1**	**-2**	**-3**	**-4**
Attentes claires					x			
Rétroaction adéquate				x				
Guides adéquats/pertinents								
Système de gestion performant					x			
Ressources								
Matériel/Outils		x						
Temps					x			
Procédés/procédures claires					x			
Environnement organisé et sécuritaire				x				
Incitatifs								
Financiers					x			
Autres types d'incitatifs					x			
Travail enrichissant			x					
Environnement de travail positif			x					
Motivations								
Motivations alignées avec le travail		x						
Employés désirent performer		x						
Attentes réalistes					x			
Recrutement/sélection des bonnes personnes (compétentes)			x					
Capacité								
Capacité d'apprendre		x						
Capacité d'effectuer ce qui est demandé		x						
Recrutement/sélection des bonnes personnes (compétentes)		x						
Limitations émotionnelles				x				
Connaissance								
Connaissances nécessaires						x		
Habiletés nécessaires				x				
Compétences liées au poste				x				
Positionnement approprié?								
Formation croisée (par les pairs)					x			
Notes :								

VI. Liste des documents et vidéos sur l'intranet

1. Politique ministérielle de sécurité de l'information. (2020).
2. Charte du bon utilisateur des actifs informationnels. (2015).
3. Directive gouvernementale en sécurité de l'information gouvernementale.
4. Directive ministérielle sur l'attribution des postes de travail mobiles. (2018).
5. Directive ministérielle sur l'utilisation des postes de travail mobiles. (2018).
6. Guide de déclaration des incidents. (2020).
7. Directive ministérielle de l'utilisation du courriel, collecticiel et Internet. (2004).
8. Procedure_mdp_teletravail2.pdf. (2021).
9. Procedure_mdp_bureau2.pdf. (2021).
10. Chroniques informatiques et vidéos :
    a. Hameçonnage. (2018).
    b. La chasse aux pourriels. (2018).
    c. Sécurité, affaire de tous. (2018).
    d. Pssi_securite_information_bulletin-2.pdf. (2020)
    e. Pssi_securite_information_bulletin-3.pdf .(2020).
    f. Plan directeur en ressources informationnelles 2019-2023.
11. Sécurisation des courriels destinés à l'externe avec FortiMail : guide de l'utilisateur. (2012).
12. Programme de sensibilisation à la sécurité de l'information. (2020).

VII. Grille d'observation

Nom, prénom de l'apprenant :
Nombre d'années dans l'organisation:
Organisation et direction :
Semaine du …….2022 au …….2022

Étape 1 : Connaissance des apprenants	**Cochez la case de notation appropriée**					**Observation ou commentaire**
Connaissances acquises observables après la formation sur les énoncés suivants	**1**	**2**	**3**	**4**	**5**	
Identifier ses rôles et responsabilités de détenteur de l'information en matière de sécurité de l'information						
Identifier les attentes de cette organisation en matière de sécurité de l'information						
Identifier les enjeux de sécurité entourant son mandat de détenteur de l'information						
Décrire en quoi consiste l'imputabilité du détenteur en matière de sécurité de l'information						
Savoir quand se référer à la Direction des technologies de l'information						
Identifier un actif informationnel						
Catégoriser l'information selon sa disponibilité, son intégrité et son niveau de confidentialité						
Identifier les étapes de test de nécessité de l'utilisation des données sensibles						
Étiqueter les données sensibles selon leur niveau de sensibilité						
Utiliser un mot de passe multifactoriel pour chaque actif						
Vérifier en continu les accès aux systèmes d'information						
Vérifier l'avancement des travaux de mise à jour et à niveau des différents systèmes						
Expliquer aux employés les directives de protection des informations sensibles						
Déclarer tout incident de sécurité à l'équipe informatique.						
Recadrer des employés pour des erreurs commises dans le traitement des données sensibles						

Étape 2 : Performance des apprenants	Cochez la case de notation appropriée					Observation ou commentaire
Capacités observables d'un détenteur après la formation sur les énoncés suivants	1	2	3	4	5	
Il définit son rôle au sein de cette organisation en matière de sécurité de l'information adéquatement[5]						
Il distingue l'ensemble de ses rôles et responsabilités par rapport à ceux des autres gestionnaires						
Il identifie tous les actifs informationnels sous sa gouverne						
Il gère systématiquement l'information tout au long de son cycle de vie						
Le test de nécessité d'utilisation des données sensibles est effectué dans 100 % des cas						
Toutes les informations sont bien catégorisées selon leur disponibilité, leur intégrité et leur niveau de confidentialité attribué, selon le cas						
100 % des informations selon leur niveau de sensibilité sont étiquetées						
Toutes les mesures de sécurité mises en place sont adéquatement[6] vérifiées						
Un mot de passe multifactoriel est utilisé pour 100 % des connexions, pour chaque actif						
Les accès octroyés pour chaque système d'information sont vérifiés chaque mois						
L'avancement des travaux de mise à jour et à niveau des différents systèmes est vérifié mensuellement						
Le respect des mesures de sécurité de l'information est vérifié						
Les directives de protection des informations sensibles sont expliquées systématiquement aux employés						
100 % des cas suspects et incidents de sécurité sont déclarés immédiatement à l'équipe informatique						
Les employés sont recadrés pour chaque erreur commise dans le traitement des données sensibles						

[5] Selon les rôles et responsabilités décrites dans la PSI.
[6] Selon les standards définis dans la PSI.

Légende des critères de notation

Étape 1	Explication
Notation	Critères d'évaluation des connaissances acquises
1	100 % des éléments sont identifiés (excellente compréhension de cet énoncé)
2	80 % des éléments sont identifiés (très bonne compréhension de cet énoncé)
3	70 % des éléments sont identifiés (bonne compréhension de cet énoncé)
4	60 % des éléments sont identifiés (compréhension à renforcer chez l'apprenant sur cet énoncé)
5	Moins de 50 % des éléments sont identifiés (faible compréhension de cet énoncé à renforcer davantage chez l'apprenant)

Étape 2	Explication
Notation	Critères d'évaluation de la performance des apprenants
1	100 % des éléments appris sont mis en application (performance très satisfaisante de l'apprenant sur cet énoncé)
2	80 % des éléments appris sont mis en application (performance satisfaisante de l'apprenant sur cet énoncé)
3	70 % des éléments appris sont mis en application (performance plutôt satisfaisante de l'apprenant sur cet énoncé)
4	60 % des éléments appris sont mis en application (performance peu satisfaisante de l'apprenant sur cet énoncé)
5	Moins de 50 % des éléments appris sont mis en application (performance insatisfaisante de l'apprenant sur cet énoncé)

10. BIBLIOGRAPHIE

Chevalier, R. (2003). « Updating the behavior engineering model », *Performance Improvement*, 42 (5), 8-14. https://doi.org/10.1002/pfi.4930420504

Deville de Periere, D. (2013). « Les enjeux de la sécurité de l'information dans le monde économique », *Marché et organisations*, (18), 19-23. https://www.cairn.info/revue-marche-et-organisations-2013-2-page-19.htm

Fondation canadienne pour l'audit et la responsabilisation. (2018). Pleins feux sur la sécurité des technologies de l'information. Vigie-Audit. https://www.caaf-fcar.ca/fr/pleins-feux-sur-la-securite-des-technologies-de-l-information

Gouvernement du Québec. (2014). Cadre gouvernemental de gestion de sécurité de l'information. https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_securite_information.pdf

Gouvernement du Québec. (2021). Rapport annuel de Gestion 2020-2021.

Gouvernement du Québec. (s.d.). Programme de sensibilisation à la sécurité de l'information, intranet de cette organisation gouvernementale.

Guérin, M. (s.d.). Modèle ADDIE. https://www.marelizeguerin.com/processus-2/modele-addie/