Suivons le guide !

Fiche synthèse

Mai 2023

SÉCURITÉ DE L'INFORMATION

Gestion de la sécurité de l'information

La sécurité de l'information vise à protéger la disponibilité, l'intégrité et la confidentialité de l'information organisationnelle. Elle touche l'ensemble de l'information de toute nature et sous toutes ses formes (papier, numérique, appareil électronique, poste et serveur informatique, verbal, etc.).

Tout le personnel, notamment les intervenants de la santé et des services sociaux, utilise et partage une grande quantité d'informations cliniques, personnelles et administratives au quotidien : dossiers d'usagers, résultats de laboratoire, diagnostics, imageries, etc. Des mesures d'encadrement sont mises en place afin d'assurer la sécurité de la gestion des renseignements confidentiels et réduire le risque de menaces telles que les virus informatiques, les attaques de pirates informatiques, les fuites d'information, les pannes d'assistance et les erreurs de manipulation.

Gouvernance en sécurité de l'information

Politiques et directives

Un ensemble de politiques, de directives et de cadre de gestion encadrent la sécurité de l'information au CIUSSS de la Capitale-Nationale :

- Politique relative à la sécurité de l'information (PO-13)
- Politique relative à la tenue du dossier de l'usager et la protection des renseignements personnels (PO-22)
- Directive relative à la consultation et à l'accès au dossier de l'usager (PO-22-2)
- Directive relative à l'utilisation des postes informatiques, de l'internet et du courriel
- Cadre de gestion de la sécurité de l'information (PO-24)
- Foire aux questions (FAQ) sur le cadre de gestion de la sécurité de l'information

Mise à jour et application de la politique

Au CIUSSS de la Capitale-Nationale, une équipe responsable de la gestion de la sécurité de l'information veille à la mise en place de mesures, afin de sécuriser les données personnelles et confidentielles de l'organisation. Cette équipe est composée du président-directeur général (PDG), du chef de la sécurité de l'information organisationnelle (CSIO) anciennement appelé responsable de la sécurité d'information (RSI), du chef adjoint de la sécurité de l'information organisationnelle (CSIO adjoint) anciennement appelé conseiller en gouvernance de la sécurité de l'information (CGSI) et du coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) anciennement appelé officier de la sécurité de l'information (OSI). Ceux-ci ont pour mandat d'assurer la mise en œuvre et l'application de la politique, du cadre de gestion de la sécurité de l'information et des directives sous-jacentes.

La définition de chacune de ces fonctions en sécurité de l'information est décrite dans la PO-13.

Sensibilisation et formation en ligne

Puisque la sécurité de l'information touche l'ensemble du personnel, **chaque employé a un rôle à remplir afin d'éviter des comportements pouvant entrainer des conséquences néfastes.** À cet effet, des capsules de formation sur la sécurité de l'information sont disponibles sur la plateforme ENA du MSSS, et ce, pour l'ensemble du personnel de l'établissement. Exemples :

- Cybersécurité : mission possible;
- Programme de sensibilisation en sécurité informationnelle;
- Confidentialité et sécurité de l'information;
- Etc.

Québec

Mise à jour du Registre d'autorité des actifs

L'équipe de la sécurité de l'information, s'assure de maintenir à jour le Registre d'autorité des actifs informationnels. Celui-ci regroupe les différents systèmes et le nom des détenteurs et des pilotes. Le registre permet de mieux répondre aux exigences de l'organisation en matière de sécurité de l'information.

Architecture en sécurité

L'équipe de la sécurité de l'information peut accompagner et conseiller les détenteurs dans leurs responsabilités en ce qui a trait à la protection des actifs et des données sous leur gouverne, notamment pour les travaux liés à :

- la catégorisation des actifs informationnels sur le plan de la disponibilité, de l'intégrité et de la confidentialité;
- l'analyse de préjudices;
- l'analyse de risques;
- la définition de plans de continuité des affaires
- etc.

Gestion des menaces, vulnérabilités, incidents, surveillance et investigation

La gestion de la sécurité de l'information est assurée par l'équipe de la sécurité de l'information. Celle-ci reçoit et prend en charge les avis de vulnérabilités pour prévenir les attaques. Elle s'occupe aussi de la détection et de la prévention d'intrusions, de la gestion des incidents de sécurité, la gestion de l'antivirus et l'accès à Internet, selon les tâches à accomplir par chacun des utilisateurs.

Centre d'expertise de services-conseils en sécurité de l'information (CESS)

La Direction de la cyberdéfense et de la gestion des risques (DGCR) du ministère de la Santé et des Services sociaux (MSSS) a comme vision la mise en œuvre d'une approche novatrice et proactive basée sur la gestion intégrée des risques en cybersécurité liée au réseau de la santé et des services sociaux (RSSS).

Centre intégré universitaire de santé et de services sociaux de la Capitale-Nationale
Québec

À cette fin, la DGCR a confié à deux (2) établissements porteurs la mise en place de deux (2) centres d'expertise, soit :

- Le Centre d'opérationnalisation de cyberdéfense (COCD) au CISSS Chaudière-Appalaches;
- Le Centre d'expertise de services-conseils en sécurité de l'information (CESS) au CIUSSS de la Capitale-Nationale.

Pour le CESS, trois établissements associés collaborent également au mandat et aux responsabilités de l'établissement porteur pour desservir l'ensemble des régions de la province soient :

- CISSS du Bas-Saint-Laurent;
- CISSS de l'Abitibi-Témiscamingue;
- CIUSSS de l'Ouest de l'Île de Montréal.

Le mandat principal du CESS, dans un contexte de regroupement des ressources spécialisées en sécurité, est de soutenir et d'accompagner les organismes et les établissements du réseau de la santé et des services sociaux afin de leur permettre de progresser et d'atteindre un niveau de maturité adéquat en sécurité de l'information.

Des projets de toute envergure, notamment au niveau de la gouvernance (ex. : accompagnement dans l'élaboration et mise en place de politiques de sécurité, de cadres de gestion, registre d'autorités, etc.), de l'architecture en sécurité (ex. : analyse de préjudices, gestion des risques, gestion des identités, etc.) ou technologique, pourront être réalisés en offrant une qualité supérieure pour chacun des produits et des services en sécurité de l'information.

Pour toutes questions sur la sécurité de l'information

Communiquez SVP avec notre équipe de sécurité de l'information à : securite.dri.ciussscn@ssss.gouv.qc.ca.