Gestion des identités et des accès

Sécurité de l'information gouvernementale

2021

Votre gouvernement

Québec

Cette publication a été réalisée par le Secrétariat du Conseil du trésor
en collaboration avec la Direction des communications.

Une version accessible de ce document est disponible en ligne.
Si vous éprouvez des difficultés techniques, veuillez communiquer
avec le Sous-secrétariat du dirigeant principal de l'information
et de la transformation numérique du Secrétariat du Conseil du trésor
au 418 643-0875, poste 5511, option 2.

Pour plus d'information :

Direction des communications
du ministère du Conseil exécutif
et du Secrétariat du Conseil du trésor
2e étage, secteur 800
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 781-9530
Courriel : communication@sct.gouv.qc.ca
Site Web : www.tresor.gouv.qc.ca

Dépôt légal – Juillet 2021
Bibliothèque et Archives nationales du Québec
ISBN 978-2-550-89885-6 (version électronique)

Table des matières

Introduction à la gestion des identités et des accès (GIA)

Qu'est-ce que la GIA?

« La gestion des identités et des accès informatiques[1] est un contrôle de première importance en matière de sécurité de l'information. Il s'agit de déterminer qui a accès à quelle information pendant une période donnée. »[2]

La GIA est un processus complexe qui intègre différentes règles, procédures et technologies. De ce fait, elle nécessite la contribution de toutes les entités administratives d'un organisme public. Fondamentalement, la GIA est basée sur les principes du **droit d'accès minimal**[3] et de **séparation des tâches**[4].

À défaut d'un encadrement adéquat de la GIA, un organisme peut s'exposer à des risques de sécurité de l'information tels que :

- Risque d'utilisation illicite d'un accès à la suite du départ de l'organisme d'un employé

  Une personne pourrait avoir accès aux systèmes, alors que cela ne devrait plus être le cas.

- Risque de destruction ou de modification de données, sans autorisation

  Un administrateur de base de données a le privilège d'altérer les données, et ce, sans qu'un contrôle soit effectué.

- Risque de fuite de données confidentielles

  Un utilisateur possède les accès lui permettant de télécharger une base de données alors qu'aucun contrôle n'est en place pour l'encadrement de cette activité.

Droit d'accès minimal

« Droit d'accès restreint afin que l'utilisateur puisse n'accomplir avec celui-ci que les seules tâches autorisées et nécessaires à l'exercice de ses fonctions. »

Séparation des tâches

« Procédure de contrôle consistant à attribuer à des personnes différentes des responsabilités relatives à l'autorisation et à l'enregistrement des opérations et à la garde des actifs afin de réduire les possibilités qu'une même personne puisse commettre et dissimuler des erreurs et des fraudes dans le cadre normal de l'exercice de ses fonctions. »

[1] Le vérificateur général du Québec parle de « gestion des identités et des accès informatiques », tandis que le Secrétariat du Conseil du trésor a publié le « Guide sur les accès logiques ». Ces termes sont équivalents.
[2] Vérificateur général du Québec (2020). Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2020-2021.https://www.vgq.qc.ca/Fichiers/Publications/rapport-annuel/163/vgq_tome-juin2020_ch02_web.pdf. Consulté en ligne le 11 mai 2021.
[3] Office québécois de la langue française. « Fiche terminologique – droit d'accès minimal ». http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=2074701. Consulté en ligne le 11 mai 2021.
[4] Office québécois de la langue française. « Fiche terminologique – séparation des fonctions ». http://gdt.oqlf.gouv.qc.ca/ficheOqlf.aspx?Id_Fiche=504988. Consulté en ligne le 11 mai 2021.

- Risque d'usurpation des accès par une personne autre que celle autorisée

  Une personne connaît l'identifiant d'un collègue et son mot de passe, et les utilise afin d'effectuer des transactions illicites.

Les objectifs

La GIA a pour objectifs de gérer et de contrôler les accès aux ressources informationnelles par des personnes ou des dispositifs (entendu comme toutes formes d'appareil, par exemple un serveur ou un téléphone cellulaire). Elle vise également à préciser les règles à observer en matière d'identification, d'authentification et d'autorisation d'accès des personnes ou des dispositifs. La GIA contribue à assurer la confidentialité, l'intégrité et la disponibilité de l'information en précisant qui peut accéder à quoi et de quelles façons. À titre d'exemples, elle contribue à réduire :

- La destruction ou l'effacement non autorisé de l'information;
- Les modifications accidentelles ou volontaires de l'information;
- Les divulgations accidentelles ou involontaires de l'information.

Les principaux volets du processus de GIA

Pour être efficace, la GIA doit s'inscrire dans un processus d'amélioration continue reposant sur quatre volets.

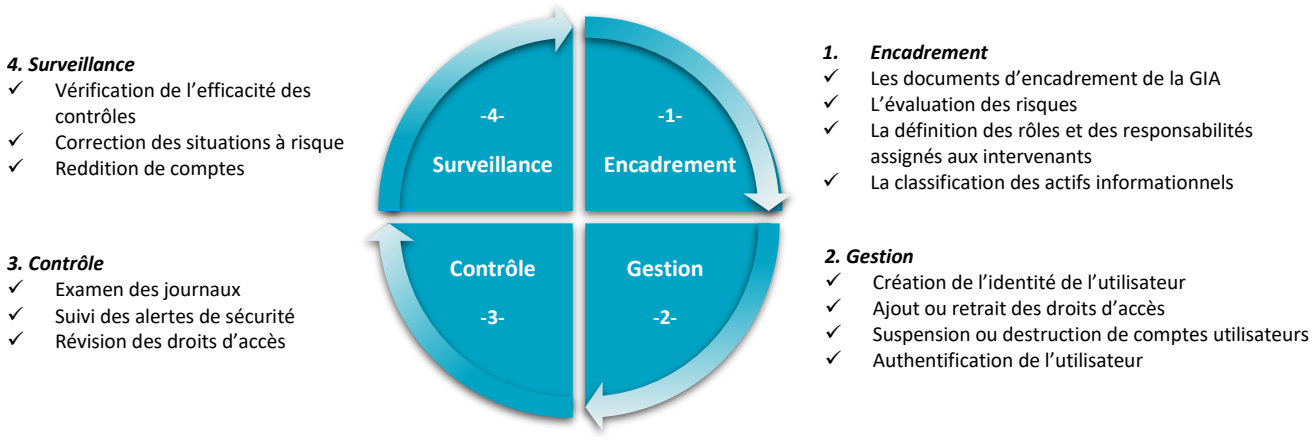
Encadrement : Proposer un ensemble d'éléments sur lequel prend appui la GIA. Il est essentiel que l'organisme classifie les informations qu'il détient, évalue ses risques de sécurité, définisse les rôles et responsabilités des différents intervenants afin d'assurer une répartition des tâches adéquates et fournisse des procédures détaillées.

Gestion : Réaliser les actions en lien avec les identités et les droits d'accès. La GIA doit permettre de préciser les règles à observer en matière d'identification, d'authentification et d'autorisation d'accès des personnes ou des dispositifs aux ressources informationnelles de l'organisme. La GIA assure l'équilibre entre la protection de l'information que l'organisme détient et l'octroi des accès et des privilèges aux utilisateurs pour qu'ils puissent travailler efficacement.

Contrôle : Assurer que la GIA est efficace et sécuritaire. Les normes internationales reconnaissent l'importance de revoir régulièrement les droits d'accès accordés aux utilisateurs, par opposition aux droits autorisés, afin de détecter et de corriger les écarts constatés lors des opérations courantes.

Surveillance : Vérifier que les contrôles sont en place et fonctionnent adéquatement. Il est important d'identifier et de corriger les situations à risque qui pourraient compromettre l'efficacité de la GIA. En faisant une reddition de comptes auprès des autorités de l'organisme, ces derniers veillent au respect des objectifs et des priorités préalablement définis ou s'assurent que les ajustements nécessaires pour maintenir en place une GIA efficace et sécuritaire soient effectués.

La figure suivante présente une vue simplifiée des principaux volets du processus de GIA.



L'importance d'assurer la reddition de comptes de la GIA

Pourquoi est-ce important de faire une reddition de comptes au regard de la GIA?

La reddition de comptes permet d'assurer un contrôle rigoureux des procédures établies afin d'éviter que les risques se concrétisent et impactent les opérations de l'organisme. La reddition de comptes consiste à faire une révision approfondie des différentes procédures, à détecter les anomalies et à apporter les correctifs nécessaires.

Le choix d'indicateurs de gestion adaptés au contexte de l'organisme peut servir à mettre en évidence l'efficacité de certains points de contrôle spécifiques portant notamment sur les aspects suivants :

- La séparation des tâches incompatibles : Démontrer la séparation des tâches des intervenants adaptée aux règles d'accès de l'organisme et en adéquation avec les exigences de la tâche.
- La révision des accès : Démontrer que la gestion des droits d'accès est appliquée rigoureusement à la suite d'un changement survenu dans le contexte de travail d'un employé (affectation, mutation, promotion, changement de fonction, etc.). Ce point de contrôle doit également couvrir les autorisations liées aux comptes avec privilèges.
- La journalisation et le suivi : Démontrer qu'une journalisation est en place, qu'elle enregistre les activités de l'utilisateur, les exceptions, les défaillances ainsi que les événements liés à la sécurité de l'information et qu'un suivi de ces journaux est réalisé. Les activités des comptes avec privilèges doivent également être journalisées.

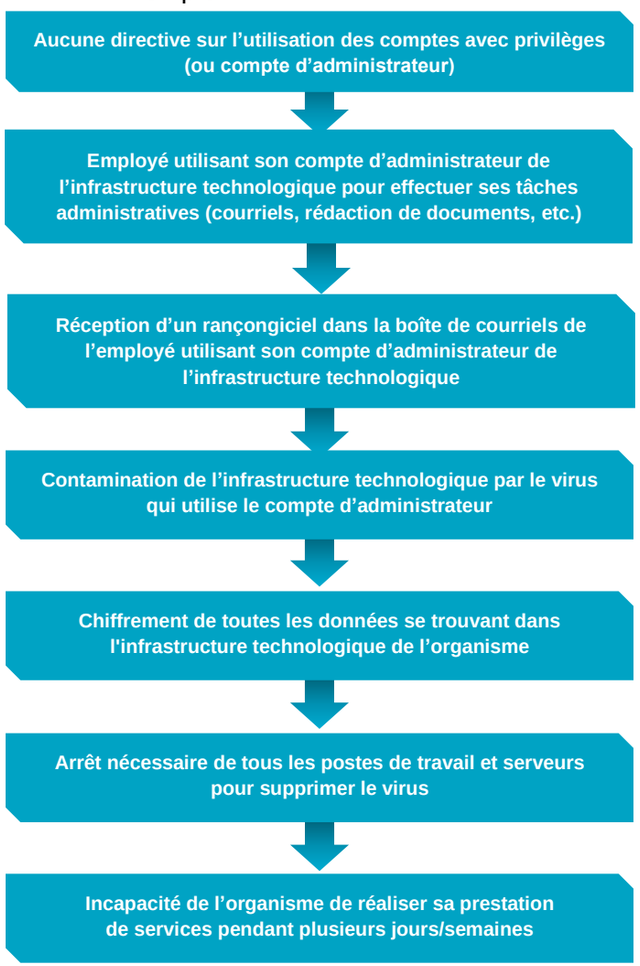
- Les paramètres des mots de passe : Démontrer que des exigences sont en place concernant les paramètres et la gestion des mots de passe.
- La révocation des accès : Démontrer que les droits d'accès à la suite du départ d'un employé sont suspendus ou supprimés et que son compte utilisateur n'est plus actif.

Comme démontré graphiquement à la page suivante, les impacts d'un processus de GIA déficient peuvent être très importants pour l'organisme et ses parties prenantes.

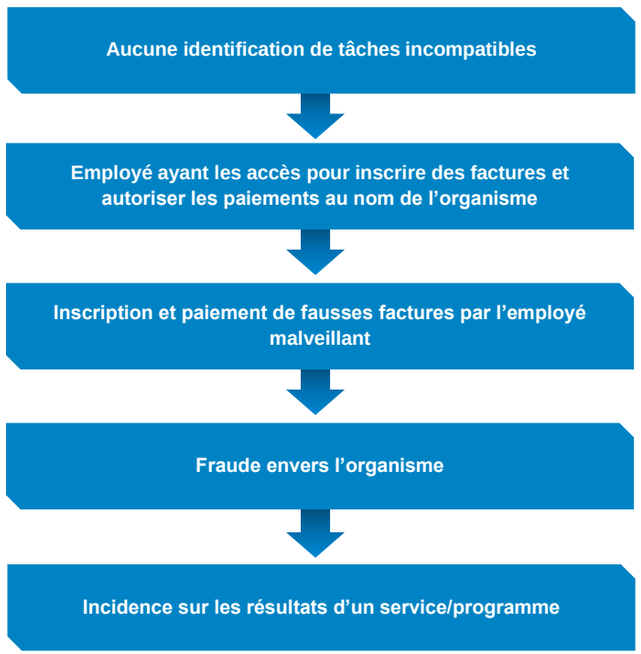
La reddition de comptes permet d'apprécier l'application du processus de GIA et, le cas échéant, d'appliquer des mesures pour corriger toutes défaillances possibles durant les opérations courantes.

Exemples d’impacts potentiels d’un processus de GIA déficient

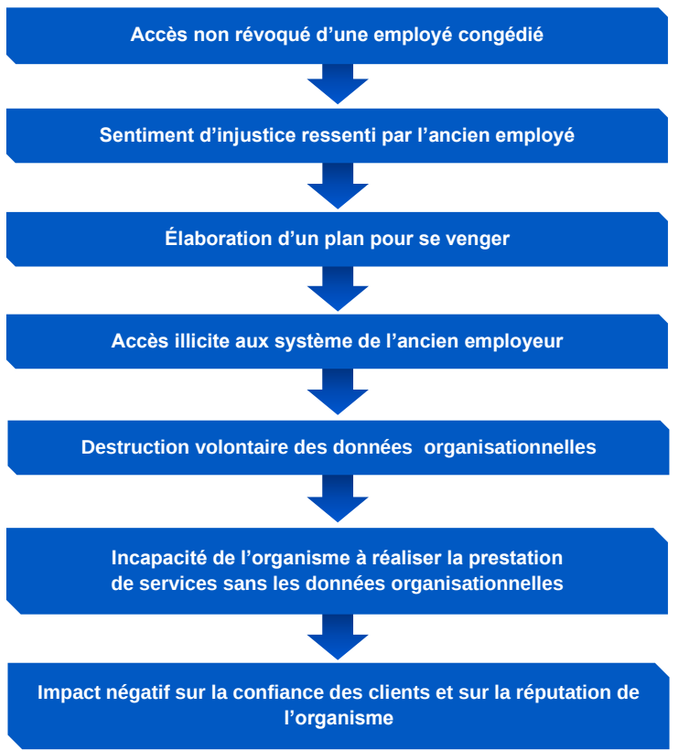
Exemple 1 : Droit d’accès minimal



Exemple 2 : Séparation des tâches



Exemple 3 : Droits d’accès non révoqués



Les éléments à aborder dans la reddition de comptes

À qui s'adresse la reddition de comptes?

La reddition de comptes des pratiques de GIA est présentée au comité chargé de la sécurité de l'information, le cas échéant, et à la haute direction. Elle permet l'appréciation du processus et des mesures de sécurité mises en œuvre pour contrôler les risques liés à la GIA, et permet de s'assurer que les objectifs et les priorités demeurent appropriés.

La fréquence optimale

La reddition de comptes doit minimalement être réalisée une fois par année. La périodicité de l'exercice peut toutefois varier en fonction des besoins et des particularités propres à chaque organisme.

L'arrimage de la reddition de comptes de la GIA aux mécanismes de reddition de comptes existants en sécurité de l'information en simplifie l'exécution et la présentation aux autorités.

Les indicateurs de gestion

Les données issues des indicateurs de gestion sont un intrant important à la reddition de comptes. Les indicateurs de gestion contribuent non seulement au suivi de l'atteinte des objectifs stratégiques de l'organisation et des cibles fixées, mais également à l'évaluation et au suivi de la performance des processus organisationnels. Par la démonstration d'amélioration ou de dégradation, d'augmentation ou de diminution sur plusieurs périodes, ils permettent d'apprécier l'efficacité des processus ou de détecter des situations à risque. Ainsi, leur analyse permet de dégager des tendances et peut aider la haute direction à déterminer les opportunités d'amélioration.

Des exemples d'indicateurs de gestion en matière de GIA sont présentés à l'annexe 1.

La présentation de la reddition de comptes

Ce n'est pas parce que la GIA est complexe que la reddition de comptes doit l'être. La présentation de la reddition de comptes doit être centrée sur les principaux éléments devant être portés à l'attention des autorités. La substitution d'explications textuelles par des éléments graphiques a notamment pour avantage de permettre une appropriation rapide des enjeux, d'alléger le contenu du document et d'augmenter l'attractivité et donc l'attention portée à la présentation.

Un exemple de présentation figure à l'annexe 2.

Références

Le contenu de ce document s'appuie sur les publications suivantes :

- Secrétariat du Conseil du trésor - Guide de gestion des accès logiques
- ISACA, Cobit 5 – Processus facilitants
- The Institute of Internal Auditors, Guide pratique d'audit des technologies de l'information – Gestion des identités et des accès.

Annexe 1 – Exemples d'indicateurs de gestion

Voici quelques exemples d'indicateurs de gestion en matière de GIA.

1. Délai moyen de révocation des accès

   Les accès accordés à un utilisateur doivent être révoqués dès la cessation des activités de ce dernier. Plus le délai est long, plus la probabilité d'utilisation des accès à mauvais escient est grande.

   Cet indicateur contribue à l'évaluation de la performance des activités de révocation des accès et permet l'établissement de cibles d'amélioration en fonction de la situation qui prévaut au sein de l'organisme.

2. Nombre de comptes inactifs depuis 30, 60 et plus de 90 jours

   Pour diverses raisons, il arrive que des comptes utilisateurs soient inactifs pour une période prolongée : vacances, congé de maternité ou de paternité, congé sabbatique, etc.

   Les données issues de cet indicateur sont importantes, car elles permettent de détecter les comptes inactifs notamment ceux sans justification et, conséquemment, de découvrir de potentielles lacunes dans le traitement des accès.

3. Pourcentage d'accès modifiés à la suite de la revue des accès

   Cet indicateur contribue à déceler la présence d'écarts ou de lacunes dans la complétion ou le traitement des demandes de modifications des accès par rapport au délai préconisé. Un pourcentage élevé pourrait être un indicateur de non-conformité des responsables aux pratiques organisationnelles de GIA. Plus ce pourcentage est élevé, plus il démontre la pertinence de faire une revue périodique des accès.

4. Nombre de comptes avec privilèges d'administration du domaine par rapport au nombre de comptes avec privilèges d'administration locaux

   Les comptes disposant d'accès privilégiés permettant d'administrer le domaine de l'organisme sont très prisés des cybercriminels, car ils permettent l'accès et la gestion de l'ensemble des ressources informationnelles. Les bonnes pratiques de sécurité de l'information recommandent d'appliquer le principe de séparation des tâches en limitant les accès accordés aux administrateurs aux systèmes pour lesquelles ils sont désignés pilotes.

   Cet indicateur permet ainsi de connaître facilement le taux de comptes avec privilèges d'administration du domaine pour ensuite les analyser et, si le besoin n'est pas justifié, rectifier la situation à risque en retirant les accès jugés superflus.

5. Nombre de comptes génériques avec privilèges

L'octroi d'accès privilégiés à des comptes génériques n'est pas recommandé par les bonnes pratiques de sécurité de l'information notamment parce qu'il est difficile d'assurer la traçabilité, et donc l'imputabilité, des actions posées à partir de ce type de comptes.

La connaissance du nombre de comptes génériques ayant des accès privilégiés dans l'organisation contribue à l'évaluation du niveau de risques liés à cette pratique et d'en atténuer la gravité par des actions correctives ou par des mesures de sécurité compensatoires si cela est jugé nécessaire.

Annexe 2 – Exemple de présentation

Bilan annuel

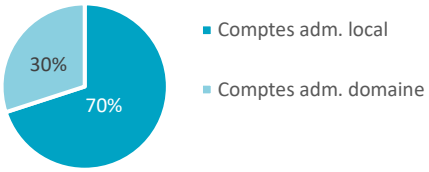
SÉCURITÉ DE L'INFORMATION

Indicateurs de gestion en matière de GIA

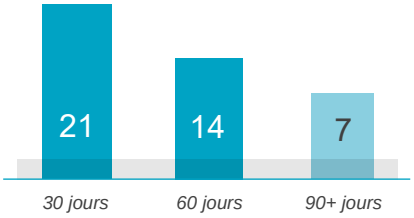
« La gestion des identités et des accès informatiques est un contrôle de première importance en matière de sécurité de l'information. Il s'agit de déterminer qui a accès à quelle information pendant une période donnée. »[1].

1. Délai moyen de révocation des accès

2. Nombre de comptes administrateur de domaine vs nombre de comptes administrateur local



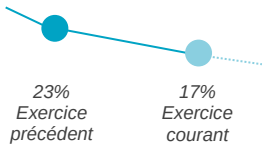
3. Nombre de comptes inactifs depuis 30, 60 et 90+ jours

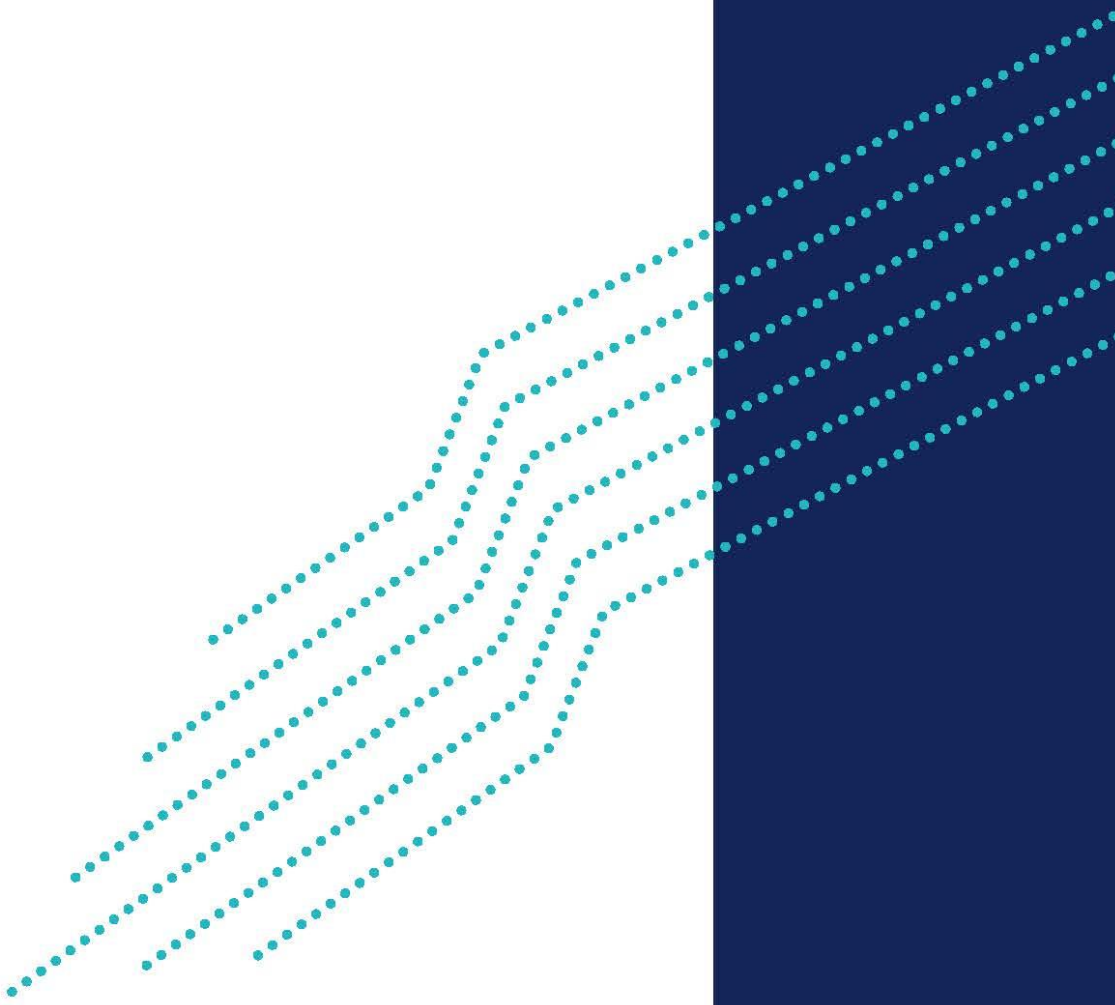


4. Nombre de comptes génériques ayant des accès privilégiés

9	14
Exercice courant	*Exercice précédent*

5. Pourcentage d'accès modifié à la suite de la revue des accès





Secrétariat
du Conseil du trésor
Québec