Mis à jour le : 1er mai 2025

La sécurité à **la GRICS**

Direction de la Sécurité de l'information et de la Protection des Renseignements Personnels GRICS

grics

Table des matières

1. Introduction

La GRICS joue un rôle stratégique dans le développement et l'offre de solutions informatiques destinées aux organismes scolaires du Québec. À ce titre, elle poursuit une démarche d'amélioration continue visant à offrir des outils numériques performants, fiables et adaptés aux besoins évolutifs du réseau scolaire québécois.

Consciente des menaces croissantes dans le domaine de la cybersécurité, la GRICS met en œuvre des mesures robustes visant à assurer non seulement la sécurité de ses produits et services, mais également celle de son infrastructure. Par ces actions, la GRICS soutient les organismes scolaires dans leurs efforts de cybersécurité, leur permettant de se concentrer sur leur mission pédagogique.

Le présent document présente les principes directeurs, les actions concrètes ainsi que les pratiques de gouvernance adoptées par la GRICS afin de garantir l'intégrité, la confidentialité et la disponibilité des données et des systèmes.

Il vise également à présenter les mesures prises par l'organisation pour se conformer aux lois et règlements en vigueur en matière de cybersécurité et de protection des renseignements personnels, notamment la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* ainsi que la *Loi sur la protection des renseignements personnels dans le secteur privé*.

2. Gouvernance et gestion des risques

Structure de gouvernance

La GRICS s'appuie sur une structure organisationnelle clairement définie pour assurer la gouvernance de la cybersécurité, composée d'un comité de sécurité de l'information et d'une équipe opérationnelle spécialisée.

Le comité de sécurité de l'information a pour mandat de soutenir l'élaboration et le déploiement du cadre de gestion de la sécurité de l'information. Il soutient la mise en œuvre de politiques, coordonne l'élaboration de plans d'action, supervise les bilans réguliers en matière de sécurité de l'information et pilote les activités de sensibilisation et de formation. Ce comité agit également comme un forum d'échange entre les parties prenantes et assure un suivi de l'évolution des projets liés à la cybersécurité.

L'équipe dédiée à la sécurité assure quant à elle l'exécution des initiatives et des politiques de cybersécurité au sein des opérations courantes. Composée de professionnels spécialisés, incluant des analystes en sécurité et des experts en gestion des incidents, elle est responsable de la mise en œuvre des contrôles techniques, de la surveillance continue des systèmes et de la réponse aux incidents. L'équipe collabore de manière étroite avec les autres départements de l'organisation afin d'intégrer les principes de cybersécurité à l'ensemble des activités de la GRICS.

Cadre normatif et politiques internes

Conformément aux exigences des lois applicables en matière de protection des renseignements personnels, la GRICS s'est dotée des politiques, procédures et directives internes nécessaires afin

d'assurer une gestion rigoureuse et conforme des renseignements personnels sous sa responsabilité.

Ces documents encadrent la collecte, l'utilisation, la communication, la conservation et la destruction de ces renseignements, et sont appliqués à l'échelle de l'organisation. Ils permettent à la GRICS d'assurer :

- Un traitement conforme aux principes de légalité, de proportionnalité et de finalité ;
- La mise en place de mesures de sécurité appropriées selon la sensibilité des données traitées ;
- L'exercice effectif des droits des personnes concernées, incluant les droits d'accès, de rectification et de retrait du consentement, le cas échéant.

Ils sont revus périodiquement afin de tenir compte des modifications législatives, des meilleures pratiques en cybersécurité et de l'évolution des risques technologiques. L'ensemble de ce cadre normatif s'inscrit dans une approche proactive, soutenue par le comité de sécurité de l'information et l'équipe opérationnelle spécialisée.

3. Sécurité des employés

Au-delà de la protection des systèmes et des données, la GRICS reconnaît que la cybersécurité repose également sur son personnel. L'engagement, la vigilance et la responsabilisation des employés constituent des éléments essentiels de notre stratégie de sécurité. À cette fin, la GRICS déploie plusieurs initiatives de formation, de sensibilisation et de contrôle préventif qui encouragent l'adoption de bonnes pratiques au quotidien.

Formation

Un programme structuré de formation est offert à l'ensemble des employés. Celui-ci couvre notamment la protection des renseignements personnels, la détection des tentatives d'hameçonnage et les bonnes pratiques en matière de cybersécurité. Les modules sont dispensés en ligne sur plusieurs semaines, de manière récurrente, et sont mis à jour annuellement afin de tenir compte des nouvelles menaces et de l'évolution des pratiques.

Campagnes de sensibilisation à l'hameçonnage

Dans le but de maintenir un niveau élevé de vigilance, la GRICS mène des simulations régulières d'hameçonnage par courriel. Ces exercices permettent aux employés de développer leur capacité à reconnaître et à signaler des tentatives de fraude ou d'ingénierie sociale.

Outil de signalement d'hameçonnage

Un mécanisme de signalement a été mis en place pour permettre aux employés d'alerter l'équipe de sécurité en cas de réception de courriels suspects. Grâce à un outil intégré à leur environnement de travail, les utilisateurs peuvent soumettre facilement les messages potentiellement malveillants à des fins d'analyse.

Vérification des antécédents

Afin d'assurer la fiabilité de toute personne accédant à des actifs informationnels sensibles, qu'il s'agisse d'employés, de consultants ou de toute autre ressource autorisée, la GRICS effectue des vérifications d'antécédents dans le cadre de son processus de recrutement. Ces vérifications

comprennent notamment la vérification des antécédents criminels, des antécédents professionnels ainsi que des références. Des réévaluations périodiques sont également effectuées pour les individus occupant des fonctions critiques ou manipulant des données sensibles, afin de maintenir un haut niveau de confiance et de conformité.

Ces vérifications sont réalisées en conformité avec les lois et règlements en vigueur en matière de protection des renseignements personnels, et les données recueillies sont traitées avec le plus haut niveau de confidentialité.

4. Sécurité des réseaux, applications et infrastructures

La sécurisation des réseaux, des applications et des infrastructures est un pilier fondamental de la stratégie de cybersécurité de la GRICS. L'objectif est d'assurer la protection continue des systèmes et des données contre les menaces, en s'appuyant sur des standards reconnus et une surveillance proactive.

Gestion des risques et référentiels de sécurité

Pour orienter ses décisions en matière de cybersécurité, la GRICS s'appuie sur des normes reconnues à l'échelle internationale. Celles-ci servent de référence pour l'identification et la priorisation des risques, notamment ceux liés aux applications web, dès les phases de conception.

Protection des postes de travail

Les postes de travail, qu'ils soient physiques ou virtuels, constituent fréquemment une porte d'entrée pour les menaces informatiques. Afin d'atténuer ce risque, la GRICS veille à ce que tous les postes et serveurs soient intégrés à un environnement sécurisé, incluant des solutions antivirus de nouvelle génération et des outils de gestion centralisée. Ces mesures assurent la traçabilité, la conformité à notre cadre normatif et un contrôle accru sur les actifs internes.

Des pares-feux sont déployés tant au niveau du périmètre du réseau qu'au niveau des postes individuels afin de contrôler le trafic réseau, prévenir les accès non autorisés et réduire les risques d'intrusions. Par ailleurs, des mécanismes de protection des applications accessibles en ligne permettent d'inspecter le trafic, de détecter les comportements malveillants et de bloquer les tentatives d'exploitation, en cohérence avec les meilleures pratiques en sécurité applicative.

Surveillance des environnements

La GRICS s'appuie sur un système centralisé de surveillance pour assurer une visibilité en temps réel sur l'ensemble de son réseau. Cette infrastructure de supervision permet l'identification rapide des anomalies, soutient les analyses d'incidents et facilite l'intervention ciblée de l'équipe de sécurité en cas d'événements nécessitant une attention particulière.

Gestion des vulnérabilités

La GRICS applique un processus itératif de gestion des vulnérabilités, reposant sur l'identification, l'évaluation, la priorisation et la remédiation systématiques des failles de sécurité découlant d'une surveillance constante de son infrastructure technologique.

Tests d'intrusion

Des tests d'intrusion sont réalisés de manière régulière, à la fois en interne et par des tiers spécialisés, afin de simuler des attaques réalistes et d'évaluer la résilience des systèmes. Ces tests

permettent de détecter d'éventuelles failles, de tester les capacités de réponse et de renforcer les contrôles existants.

5. Sécurité des données

La GRICS met en œuvre un ensemble de mesures techniques et organisationnelles visant à assurer la confidentialité, l'intégrité et la disponibilité des données. Ces mesures couvrent l'ensemble du cycle de vie de l'information, de sa collecte à sa suppression, et s'appliquent tant aux environnements internes qu'aux services rendus aux clients.

Chiffrement des données

La GRICS veille en tout temps à ce que l'ensemble des données présentes sur ses équipements, de même que celles hébergées, soient protégées au moyen de mécanismes de chiffrement robustes. Ces mécanismes sont appliqués tant lors de la transmission et du traitement des données de ses clients qu'au repos.

Contrôles d'accès

L'accès aux données est strictement encadré. Seules les personnes autorisées, en fonction de leur rôle et de leurs responsabilités, peuvent consulter ou manipuler des données sensibles. Ces accès sont révisés régulièrement afin de s'assurer qu'ils demeurent pertinents, justifiés et conformes aux politiques de l'organisation.

Protection contre l'exfiltration de données

Des dispositifs de sécurité sont en place afin de prévenir toute tentative de fuite de données, assurant leur protection même en cas d'incident ou de cyberattaque. Une équipe spécialisée assure une veille constante, incluant le web et le dark web, afin de détecter toute exposition ou tentative de compromission des données.

Redondance et sauvegardes

La GRICS a mis en place un système de sauvegarde et de réplication visant à assurer la continuité des opérations et à permettre une restauration rapide des données en cas d'incident.

- **Sauvegardes fréquentes des bases de données :** effectuées régulièrement, elles assurent une protection continue des données.
- **Sauvegardes quotidiennes des serveurs et fichiers** : tous les systèmes essentiels font l'objet de sauvegardes complètes chaque jour.
- **Stockage sécurisé** : les sauvegardes sont conservées dans des centres de données fiables, permettant un accès rapide et sécurisé en cas de besoin.
- **Réplication vers un stockage à long terme** : une fois la sauvegarde effectuée, elle est immédiatement répliquée vers un environnement de stockage à long terme. Cette redondance supplémentaire renforce la sécurité et garantit l'intégrité des données, même en cas d'incident affectant l'infrastructure principale.

Suppression sécurisée des données

Lorsque les données ont atteint la fin de leur cycle de vie, elles sont supprimées de manière sécurisée. Ce processus implique l'utilisation de méthodes de destruction des données qui empêchent tout accès ultérieur, qu'il soit accidentel ou malveillant. Nous utilisons des

algorithmes de destruction conformes aux meilleures pratiques de l'industrie, qui garantit que les données supprimées ne pourront pas être récupérées, même par des techniques de récupération avancées.

Gestion des bases de données clients et des « CSS virtuelles »

Dans le cadre de ses divers mandats, la GRICS est amenée à traiter des bases de données clients contenant des renseignements personnels ainsi que les bases de données des CSS virtuelles. Un processus strict encadre la gestion de ces données sur des environnements sécurisés et isolés. Ce processus inclut :

- La dépersonnalisation des données, lorsque requises ;
- Le suivi rigoureux de leur cycle de vie ;
- Une suppression automatisée dès que la conservation n'est plus justifiée.

6. Développement sécurisé

En tant qu'organisation spécialisée dans le développement de solutions logicielles pour le milieu scolaire, la GRICS intègre des pratiques rigoureuses de cybersécurité tout au long du cycle de vie applicatif. L'objectif est de détecter, prévenir et corriger les vulnérabilités dès la phase de conception, jusqu'à la mise en production et au-delà.

Intégration de la sécurité dans le cycle de développement

La GRICS adopte une approche intégrant les exigences de sécurité à chaque étape du développement logiciel. Cette approche repose sur plusieurs pratiques clés :

- Identification des exigences de sécurité ;
- Analyse des risques applicatifs ;
- Intégration de contrôles de sécurité ;
- Réalisation de tests tout au long du cycle de développement.

Cette méthodologie assure que les applications livrées répondent à des standards rigoureux en matière de sécurité tout en demeurant alignées sur les objectifs fonctionnels visés.

Tests de vulnérabilité

La sécurité applicative est renforcée par la réalisation régulière de tests de vulnérabilité, qui visent à identifier et corriger proactivement les failles potentielles avant qu'elles ne puissent être exploitées. La GRICS s'appuie également sur des outils d'analyse automatisée pour détecter les vulnérabilités de manière continue.

Ces pratiques assurent que les applications livrées sont conformes aux pratiques reconnues et résistent efficacement aux menaces.

7. Sécurité physique

La GRICS met en place un ensemble de mesures destinées à assurer un environnement de travail sûr et sécurisé pour ses employés, tout en protégeant l'accès physique aux installations et aux actifs informationnels sensibles.

Vidéosurveillance et contrôle des accès

Des systèmes de vidéosurveillance sont déployés à des emplacements stratégiques, conformément à une directive interne élaborée en respect des lois en vigueur en matière de protection de la vie privée. Cette directive encadre l'installation et l'utilisation des équipements afin d'en assurer un usage proportionné, transparent et justifié.

Les zones à accès restreint, notamment celles où sont traitées des données sensibles, sont clairement délimitées. L'accès à ces espaces est restreint au moyen de cartes d'accès électroniques, ne permettant l'entrée qu'aux personnes autorisées. Ce contrôle vise à prévenir les intrusions non autorisées et à garantir l'intégrité des environnements de travail.

Plan d'urgence et mesures d'évacuation

Un plan de mesures d'urgence et d'évacuation est en place afin de répondre efficacement aux situations nécessitant l'évacuation partielle ou complète des lieux. Ce plan vise deux objectifs principaux :

- Assurer la protection de la santé et de la sécurité des employés et des visiteurs ;
- Maintenir la continuité des services offerts aux clients et partenaires, même lors d'événements perturbateurs.

Centres de données et hébergement infonuagique

Les centres de données utilisés par la GRICS sont dotés de mesures de sécurité avancées. Ces installations sont protégées par :

- Une surveillance continue (24/7) ;
- Des systèmes de contrôle d'accès physique stricts ;
- Des alarmes et des dispositifs de protection contre les incendies ;
- Des inspections régulières pour assurer la conformité aux standards établis en matière de sécurité.

L'accès physique à ces centres est restreint aux personnes dûment autorisées, et toute tentative d'accès est enregistrée et surveillée. En ce qui concerne les données hébergées en infonuagique, la GRICS collabore exclusivement avec des fournisseurs reconnus afin de garantir les plus hauts niveaux de protection et de résilience des données.

8. Gestion des fournisseurs

La GRICS intègre des exigences de sécurité de l'information dès les premières étapes du processus d'approvisionnement, et maintient une vigilance tout au long de la relation avec ses fournisseurs.

Évaluation des fournisseurs

Tous les fournisseurs sont soumis à une évaluation rigoureuse visant à valider leur conformité aux bonnes pratiques et aux standards de cybersécurité reconnus. Des critères précis sont intégrés aux documents d'appel d'offres afin d'assurer que seuls les fournisseurs présentant un niveau de sécurité adéquat puissent être sélectionnés.

Clauses contractuelles

Les ententes contractuelles signées par la GRICS contiennent des clauses portant sur :

- La protection des données et la confidentialité des informations ;
- La gestion des incidents de sécurité ;
- La cybersécurité des services ou systèmes fournis ;
- Les droits d'audit, permettant à la GRICS de vérifier périodiquement la conformité des fournisseurs à ses exigences.

Encadrement des fournisseurs infonuagiques

Le recours à des services infonuagiques par la GRICS est soumis à des critères de sélection stricts. Seuls les fournisseurs infonuagiques validés par le ministère de la Cybersécurité et du Numérique (MCN) sont retenus. Ces fournisseurs doivent démontrer leur conformité à des normes de sécurité rigoureuses ainsi qu'aux exigences législatives applicables.

La GRICS assure également une surveillance continue de ces services, notamment à travers des mises à jour et des vérifications régulières.

9. Plan de continuité des affaires

La GRICS a mis en place un plan de réponse aux incidents structuré afin de permettre à ses équipes d'agir rapidement en cas d'événement compromettant la sécurité des données. Ce plan vise à rétablir les opérations dans les meilleurs délais tout en minimisant les impacts potentiels.

Gestion des incidents de sécurité

Le processus de gestion des incidents comprend les étapes suivantes :

- **Détection et enregistrement** : Identification de l'incident et consignation des éléments pertinents pour assurer la traçabilité ;
- **Classification** : Évaluation du type, de la gravité et de la portée de l'incident ;
- **Investigation** : Analyse menée par les équipes de sécurité afin d'identifier la source de l'incident, les mécanismes d'intrusion employés et les systèmes touchés ;
- **Rétablissement** : Mise en œuvre des mesures nécessaires pour un retour à la normale des services affectés.

Chaque incident est documenté, évalué et fait l'objet d'un suivi, incluant une analyse post-incident afin d'identifier les améliorations à apporter.

Mesures d'urgence et stratégies de confinement

En cas d'incident, un confinement rapide et efficace des actifs est mis en œuvre afin de limiter l'impact et de prévenir toute compromission supplémentaire de l'environnement technologique. Selon la nature de l'incident (tels que logiciels malveillants, intrusion réseau ou compromission de compte), des stratégies de confinement spécifiques, fondées sur une approche rigoureuse de gestion des risques, sont appliquées de manière proactive.

Des critères clairs permettent de déterminer le niveau d'urgence, les ressources mobilisées et les actions à mettre en œuvre pour contenir la menace.

Plan de reprise d'activité (PRA)

Une fois l'incident contenu et les causes traitées, la GRICS active son **plan de reprise d'activité (PRA)** afin de restaurer les systèmes de manière graduelle et sécurisée. Ce processus vise à :

- Réduire les délais de rétablissement des services ;
- Assurer l'intégrité des systèmes restaurés ;
- Minimiser les interruptions de service pour les utilisateurs finaux.

Le PRA est régulièrement testé et mis à jour afin de garantir son efficacité et sa conformité aux meilleures pratiques en matière de continuité des opérations.

10. Surveillance, détection et prévention des menaces

La GRICS assure une surveillance active et continue (24/7) de ses systèmes afin de détecter, analyser et répondre rapidement à toute menace.

La surveillance est assurée par une équipe de sécurité spécialisée. Cette équipe est mobilisée en permanence pour assurer :

- L'analyse des alertes ;
- La réponse rapide aux événements détectés ;
- La réalisation d'analyses approfondies en cas de compromission ou d'attaque ciblée.

En dehors des heures normales de travail, une équipe sur appel est également disponible afin de garantir la surveillance ainsi qu'une capacité d'intervention rapide en tout temps.

Automatisation de la détection et de la réponse

Afin de renforcer l'efficacité opérationnelle, la GRICS s'appuie sur des outils automatisés de détection et de réponse aux incidents. Ces systèmes permettent de :

- Identifier rapidement les comportements anormaux ou suspects ;
- Déclencher automatiquement les premières mesures de confinement ou de correction ;
- Réduire les délais de réaction et limiter l'impact des menaces ;
- Minimiser les risques liés aux erreurs humaines.

L’automatisation contribue ainsi à augmenter la capacité de réponse tout en assurant une couverture constante et fiable.

11. Engagement durable en cybersécurité

Consciente de l’évolution constante des menaces, la GRICS adopte une démarche d’amélioration continue afin de renforcer sa posture de cybersécurité. Cette approche permet à l’organisation d’anticiper les nouveaux risques et d’ajuster ses mesures de sécurité en fonction des changements technologiques ou législatifs.

Stratégie de cyberrésilience

La stratégie de cyberrésilience de la GRICS repose sur une évaluation régulière des risques, l’alignement sur les meilleures pratiques et l’intégration continue d’innovations technologiques en matière de sécurité. Elle comprend :

- La réalisation périodique d’audits internes et externes ;
- La mise à jour systématique des outils de sécurité et de son cadre normatif ;
- L’adaptation des mécanismes de défense en fonction des nouvelles menaces.

Engagement envers les employés, clients et partenaires

La GRICS s’engage à protéger les données de ses employés, clients et partenaires en mettant en œuvre des contrôles de sécurité robustes et adaptés à chaque contexte. Cet engagement se traduit par :

- La mise en place de mesures de sécurité éprouvées ;
- Une communication transparente sur ces mesures ainsi que les bonnes pratiques ;
- Des programmes de formation continue pour le personnel ;
- Une collaboration étroite avec les partenaires afin de promouvoir un écosystème numérique sécurisé, fiable et conforme aux lois et règlements en vigueur.