12/11/2025

Politique de sécurité de l'information (PSSI) Popcorn communication

Chloé Arsenault
Janie Sarrazin
César Escobar Garcia
Emilien Gagnon

Travail pour Hawa Lom

Gestion de risque

420-3CA-CB_RISK_S3B

Table des matières

Section 1 — Présentation générale de l'organisation

Popcorn communication, une grande entreprise québécoise axé sur la revente de bande passante internet fondé en 2020 de près de 250 employés et 100 000 clients qui a connu un essor fulgurant depuis sa sortie au grand public. Elle a une affiliation d'achat avec des compagnie tel que Bell, Vidéotron et Rogers.

Cette dernière vise aussi à fournir des services philanthropiques aux compagnies plus démunies en offrant des services de base à très faible coût. Nous nous engageons aussi à une association avec un grand nombre de PME afin de favoriser l'économie circulaire québécoise. Le secteur d'activité de l'entreprise se situe principalement au niveau des particuliers.

L'entreprise, qui a évolué au même rythme que ses concurrents les plus prestigieux, adopte aujourd'hui des technologies de pointe requérant les meilleures spécialistes de la province. De son siège social à Montréal, elle gère et fournit un service de qualité des plus aimé de sa clientèle. La sécurité de l'information est, et doit être, au cœur même de la coordination et des pulsions de l'entreprise.

L'entreprise compte en elle des donnés de la facturation, des données personnelles, des données clients, propriété intellectuelle ainsi que des infrastructures réseau tel que des routeurs, serveurs, câblages réseau, PDA, ordinateur de bureau, ordinateur portable et autres. Ils ont donc de nombreux enjeux à protéger.

Dans cet ordre d'idée, la collecte d'information sous toutes ses formes, ainsi que sa conservation son utilisation à des fins administratives et contractuelles représente un enjeu capital autant pour l'entreprise que pour ses clients, ainsi que pour le respect des lois en vigueur dans la province et du pays.

L'impact d'une telle manipulation doit être prise au sérieux. Toute contravention liée à la mauvaise manipulation, à une mauvaise gestion ou à une mauvaise sécurisation de tels actifs pourrait notamment entrainer des risques financiers, une perte de réputation, une perturbation sur les opérations et des pertes ou des vols de propriété intellectuelle.

[1]L'organisation doit donc mettre en place les politiques, procédures et contrôles techniques nécessaires pour gérer les risques liés à la sécurité de l'information et assurer la continuité des activités.

L'entreprise adopte cette politique de sécurité de l'information afin de définir la sécurité de ses actifs informationnel ainsi que les orientations stratégiques dans le but d'assurer la continuité des opérations de façon sécuritaire et pour la croissance de l'entreprise. Elle doit s'appuyer sur les bonnes pratiques, la conformité des normes et des règlementations.

Section 2 — Mission, vision, valeurs

Mission La mission de Popcorn Communications est de donner aux particuliers et aux entreprises les moyens de réussir. Nous veillons à ce que vos données circulent en toute sécurité et à grande vitesse. Nous offrons une bande passante internet accessible, fiable et sécurisée, favorisant la connexion et la croissance, tout en contribuant au bien-être de la communauté grâce à des services essentiels abordables.

Vision Notre vision est simple : devenir le chef de file et le fournisseur de bande passante internet le plus fiable au Québec, reconnu pour notre engagement envers les technologies de pointe, un service exceptionnel, la responsabilité sociale et le développement des PME locales.

Nos Valeurs Fondamentales

La sécurité de l'informations se traduit par le respect des normes les plus strictes en matière de sécurité de l'information et de pratiques éthiques, garantissant ainsi la confidentialité, l'intégrité et la disponibilité des données.

Transparence et **Excellence** se traduit par l'engagement de l'entreprise à fournir un service de qualité, communiquer de façon claire et compréhensible pour tous

Innovation se traduit par l'adoption et l'exploitation en permanence les technologiques de pointe pour offrir des services de qualité supérieure.

Communauté, fournir des services essentiels à faible coût aux personnes dans le besoin et collaborer activement avec les PME locales pour stimuler la croissance économique.

Croissance & développement, favoriser une croissance rapide tout en investissant dans les meilleurs talents et en encourageant la formation continue au sein de notre équipe diversifiée.

Section 3 — Enjeux informationnels

Confidentialité Avec près de 100 000 clients et une croissance exponentielle, la gestion, le stockage et l'accès efficaces à d'importants volumes de données d'utilisation de la bande passante, d'informations clients et de détails de facturation représentent un défi majeur. Avec 250 employés occupant divers postes, des contrôles d'accès insuffisants ou un manque de sensibilisation du personnel peuvent entrainer des fuites de données malveillantes.

Intégrité L'entreprise utilise un large éventail de technologies. Des formats de données incohérents pourraient engendrer des erreurs de facturation, de prestation de services ou de rapports de conformité. Il est essentiel de maintenir tous les logiciels à jour afin de corriger les vulnérabilités connues. Une négligence dans l'application des mises à jour peut créer des points d'entrée permettant aux attaquants de compromettre l'intégrité du système et des données.

Disponibilité Les mises à jour logicielles et les mises à niveau matérielles doivent être soigneusement planifiées et exécutées afin de minimiser les temps d'arrêt et d'assurer la disponibilité continue des services et des informations.

Traçabilité Bien que non explicitement mentionné, le défi que représente la « gestion du stockage et l'accès à d'importants volumes de données d'utilisation de la bande passante, d'informations clients et de détails de facturation » implique une bonne tenue des registres et la capacité de suivre les modifications et les accès à des fins de responsabilisation, éléments fondamentaux de la traçabilité dans les systèmes complexes.

Conformité légale et réglementaire Conformité à toutes les lois provinciales à la collecte, au stockage et à l'utilisation des données pour une clientèle aussi importante, notamment en ce qui

concerne les informations personnelles et d'utilisation sensibles, exige une vigilance et une adaptation constantes.

Réputation et confiance Toute violation peut avoir de graves conséquences, notamment une atteinte à la réputation et une érosion de la confiance des clients, deux aspects critiques pour une entreprise comptant 100 000 clients.

Valeur économique de l'information Les risques financiers et la perte de propriété intellectuelle témoignent de la valeur économique élevée des informations protégées.

Section 4 — Champ d'application de la politique

La présente politique de sécurité de l'information s'applique à :

Employés, contractants, intérimaires, fournisseurs, partenaires tiers ayant accès aux actifs informationnels de l'entreprise ainsi qu'à tous les clients affiliés à l'entreprise.

L'information visée par la présente politique est :

Les informations détenues et protégées par Popcorn Communication comprennent, sans s'y limiter Actif primaire et principal et Actif de support:

- Processus d'affaire et activités de l'entreprise, information
- Matériel, logiciel, réseau, personnel, site et structure de l'organisation
- Les informations créées, reçues, stockées, traitées en transit par Popcorn Communication
- Les données clients, les informations de facturation, la propriété intellectuelle et les communications internes
- L'ensemble des systèmes d'information, réseaux et infrastructures détenus ou gérés par Popcorn Communication ;
- Les logiciels propriétaires tels que Popcorn UI et les technologies tierces (Microsoft, Fortinet, Splunk).

Activités visées par la politique :

Toute activité impliquant l'utilisation, la transmission, l'inférence ou le stockage de renseignements, sous quelque forme, format ou lieu que ce soit, est visée par la présente politique. Celle-ci vise à assurer la conformité à la Loi sur la protection des renseignements personnels dans le secteur privé du Québec et aux autres lois provinciales et fédéral applicables en matière de protection des données.

Section 5 — Cadre légal et normatif

Le cadre légal et normatif constitue la base de la PSI de Popcorn communication. L'entreprise offre des services de fibre optique et un service IOT pour plus de 100 000 abonnées. Nous nous assurons de respecter les lois et règlements en vigueur au Québec et au Canada ainsi que les lois spécifiques

à notre secteur, tel que la loi sur les télécommunications (LC 1993, ch.38). Nous intégrons également des normes internationales certifiables comme l'ISO 27001. Cela assure la conformité règlementaire, une gestion des risques efficace pour ainsi protéger nos actifs critiques. Nous nous référons aux normes ISO, NIST et CIS-CSC dans chacune des sphères de la sécurité de l'information, entre autres mais sans s'y limiter, pour la gouvernance, les principes directeurs, inventaires et classification des actifs, analyse et traitement du risques et la réponse aux incidents. Pour un guide plus complet de nos utilisations des lois règlementaires et normes, veuillez-vos référer à l'annexe XII. Ces lois et normes permettent d'assurer le respect des exigences du secteur des télécommunications et de prendre en compte les menaces actuelles telle que les attaques par déni de service distribué (DDoS), qui constituent un défi majeur dans le milieu des télécommunications.

Section 6 — Principes de sécurité

Dans le but de garantir des efforts soutenus envers la confidentialité, disponibilité et l'intégrité des informations, Popcorn communication utilise entres autres la philosophie DevSecOps au niveau du développement et adopte plusieurs autres principes qui sont encré dans l'identité de l'entreprise au niveau de la sécurité général.

Philosophie DevSecOps L'entreprise adopte la philosophie DevSecOps pour l'ensemble des activités lié au développement. Cette approche garantit que les principes de sécurité, tels que la confidentialité, l'intégrité et la disponibilité, sont pris en compte dès le début du développement. Les concepts de détection, d'analyse et de correction de vulnérabilités sont au cœur de cette approche.

Principe du premier point de contact Les entreprises de télécommunications sont souvent ciblées par des tentatives d'hameçonnages visant à soutirer les renseignements personnels aux utilisateurs. Popcorn communication a mis en place un principe de premier point de contact pour les employés et utilisateurs en optant pour une stratégie de première ligne anti-hameçonnage. Les techniciens informatiques agissent comme première ligne de défense. L'entreprise assure la disponibilité 24/7 d'une équipe qualifiée afin que chaque employé ou utilisateur ait un accès direct à un spécialiste en tout temps, car nous savons que chaque minute compte. Cela permet à la fois de prévenir et d'appliquer des correctifs de façon structurée, contrôlée et rapide.

Principe « Approche Zéro-Trust (aucune confiance) » Le principe *Zéro Trust* est une collection de concepts qui a pour but de minimiser l'incertitude et renforcer l'exactitude. Cela comprend, entre autres, le *Zéro Trust* au niveau du contrôles des accès en adoptant la méthode du moindre privilège. Nous utilisons également le MFA obligatoire pour tous les comptes, y compris les admins et une interdiction totale du partage des accès. Nous utilisons également le principe *Zéro Trust* au niveau du réseau interne de l'entreprise en segmentant nos réseaux, en appliquant des règles très restrictive au niveau des pare-feu (deny all, allow by exception, en appliquant une politique de chiffrement obligatoire, en évaluant la fiabilité des partenaires ou fournisseurs, entre autres. *Réf. Nist SP-800-207 Zéro Trust Architecture.*

Principe défense en profondeur Popcorn communication ne veut pas dépendre d'une seule couche de protection pour la protection de ses actifs informationnels. C'est pourquoi elle opte la protection multicouche afin d'offrir une meilleure protection en combinant plusieurs méthodes protectives. Par exemple, pour l'hameçonnage, nous utilisons plusieurs couches protectives afin de contrer cette attaque. Nous avons une couche organisationnelle (incluant une formation et sensibilisation), une couche sur le contrôle des accès (incluant l'utilisation du MFA, gestion des identifiants), une couche technique au niveau de la détection (incluant la détection de malware, intrusion) et une couche de réponse rapide aux incidents.

Section 7 — Gouvernance

Leadership Popcorn communication s'engage à faire preuve de leadership en affirmant son engagement en faveur du système de gestion de la sécurité de l'information. L'entreprise s'assure qu'une politique et des objectifs sont en places, conformément à leurs exigences en matière de sécurité et conformément à son guide normatif. Elle s'assure également que les pratiques mises en place sont compatibles avec ses valeurs stratégiques. Elle veille à fournir toutes les ressources nécessaires à la mise en place du système de gestion de sécurité et que le système de gestion de sécurité produit les résultats attendus. Elle démontrera l'importance de l'efficacité et de l'amélioration en continue du système de gestion de l'information en guidant, encourageant et aidant les dirigeants du système afin de contribuer à la sécurité de l'information.

Planification et amélioration continue (PDCA) L'entreprise met en œuvre des plans d'actions pour protéger son système informationnel de façon continuelle. Entre autres. elle *planifie* et implémente l'identification de ses risques, *mets en place* des systèmes de sécurité, elle *évalue* la conformité et ses résultats et elle *corrige* toute failles détecter afin de renforcer continuellement son système de gestion de la sécurité de l'information.

Rôles et responsabilités Afin de garantir l'établissement d'un système de sécurité de l'information performant et sécuritaire, il est impératif d'identifier les rôles clés essentiels ainsi que les responsabilités de ceux-ci. Pour le tableau complet, voir l'Annexe IV – Organigramme de sécurité.

Chef exécutif (CEO) Son rôle principal envers la sécurité de l'information est de définir la vision et les attentes. Le chef exécutif a pour rôle d'approuver les politiques incluant la politique de sécurité de l'information et adopte tous les changements nécessaires à l'organisation selon les recommandations de la direction de la sécurité de l'information. Il doit également s'assurer de fournir toutes les ressources nécessaires en approuvant les budgets. Il doit promouvoir une culture de sécurité à travers l'entreprise et soutenir les initiatives de cybersécurité.

Responsable de la sécurité de l'information (CISO/ISM) Étant le principal responsable de la mise en place de la stratégie de sécurité informatique, il dirige les efforts pour protéger le système et les données contre les menaces. Il supervise toutes les enquêtes internes. Il doit établir des

rapports et des bilans annuels. Il s'assure de la protection des actifs informationnels de l'entreprise.

Analyste SOC Son mandat est d'analyser en temps réel les évènements de sécurité. Il agit de façon proactive aux menaces envers la confidentialité, disponibilité et l'intégrité. Il notifie à son responsable les incidents et accompagne le traitement des incidents. Il contribue à la mise en place du système de détection des incidents. Il collabore à l'amélioration continue des procédures.

Analyste GRC (gouvernance, risque et conformité) Il élabore la politique de sécurité. Il est responsable d'identifier les actifs informationnels, leur propriétaire, les vulnérabilités et les menaces au sein de l'entreprise. Il doit évaluer les risques pour ensuite coordonner des plans d'action, avec le département technique et son équipe, la mise en place de mesures correctives et préventives afin de protéger ses actifs informationnels selon leur priorité. Il s'assure également qu'un registre d'incident est bien en place et utilisé. Il élabore des audits de conformité et des mesures d'indicateur de performance (KPI).

Direction des finances (CFO) Il est la personne responsable au niveau des risques financiers reliés à la sécurité de l'information. Il assure qu'une attribution suffisante du budget est bien établie au niveau de la sécurité de l'information, correspondant aux valeurs stratégiques de l'entreprise.

Direction de la technologie de l'information (DTI) Le responsable du département de la technologie de l'information collabore étroitement avec la direction de la sécurité de l'information afin de mettre en place toutes les contrôles de sécurité techniques et applicatifs. Il supervise la mise en œuvre des technologies de l'information incluant les contrôles de sécurité.

Infrastructure Il est le principal responsable de la disponibilité et de la redondance dans le domaine de la sécurité de l'information. Il applique et maintient les couches de sécurité sur l'infrastructure (stockage, serveur, etc.). Il est également le responsable de l'accès physique aux salles de serveurs et autres infrastructures.

Réseau Le responsable réseau a la charge d'optimiser la connectivité et la sécurité des opérations de Popcorn communication. Étant l'administrateur des réseaux informatique, Il est en charge des systèmes de prévention et détection. Selon notre principe << zéro-trust >> il met en œuvre la segmentation réseau afin de limiter la propagation des menaces.

Support TI Le rôle du support TI est l'entretien des systèmes de l'information, application web et tous les outils de collaborations dans l'organisation. Il est le premier répondant lors des attaques d'hameçonnage ou des problèmes d'accès, selon notre principe du premier point de contact. Il sécurise les postes de travail, et applique les droits d'accès pour les utilisateurs et leurs équipements.

DevOps Le responsable DevOps est le responsable de la sécurité dans le développement dès sa conception. Il utilise la méthodologie DevSecOps pour intégrer la sécurité dans le processus de

développement logiciel. Autrement dit, il s'assure que des mesures de sécurités solides ont été introduites tout au long du cycle de développement des applications et que le code développé correspond aux exigences de Popcorn Communication. Il surveille et configure la sécurité du service On-Premise et remédie à ses vulnérabilités en s'assurant que la sécurité dans la base de code soit une priorité.

Analyse/développeur Le responsable du développement logiciel est responsable de la sécurité des applications sécuritaire dès sa conception. Il se distingue du développeur lambda. Il fait l'architecture et créé des logiciels avec les normes et bonnes pratiques en matière de développement sécuritaire. Il s'assure que lui et chacun de ses pairs suivent une méthodologie de révision de codes sécuritaires pour une meilleure traçabilité ainsi que des tests unitaires et d'intégrations solide afin de toujours garder un standard de sécurité optimal.

Direction des ressources humaines (DRH) La direction des ressources humaines est responsable de la gestion des accès et doit s'assurer d'une formation adéquate en sécurité de l'information à l'embauche et tout au long du cycle de vie de l'employé. Elle doit s'assurer que les employés n'ont accès qu'aux informations nécessaires à leur fonction et que les accès sont ajustés à la suite de tout changement ainsi que révoqué dès la fin de l'emploi en collaborant avec le département de l'information technologique. Elle doit s'assurer que la politique des ressources humaines est à jour en tout temps et que toutes les procédures et responsabilités des employés face à la sécurité de l'information soient bien indiquées et de façon claire.

Utilisateurs Tous les utilisateurs doivent respecter les politiques de l'organisation. Ils doivent protéger les actifs informationnels qui leur sont attribué. Ils sont responsables de signaler tout incident ou toute activités pouvant mettre en danger la sécurité de l'information et être particulièrement vigilant concernant les tentatives d'hameçonnages qui sont particulièrement présent dans le domaine de la télécommunication. Il doit doubler de prudence concernant l'ingénierie sociales et les logiciels malveillants. Ils doivent appliquer les contrôles de sécurités et faire preuve de bonnes pratiques en tout temps afin protéger les informations. Il doit, entre autres, utiliser des mots de passe robuste sans jamais les partager, verrouiller ses sessions dans les moments d'absence, maintenir un bureau propre et écran propre et il doit participer aux formations.

Pour plus d'informations sur la structure de gouvernance de notre entreprise, vous référez aux Annexes IV (registre d'autorité) et VI (organigramme de la sécurité).

Section 8 — Inventaire et classification des actifs

La classification des actifs a été réalisé selon les principes définis dans les normes ISO 27001 et ISO 27002 et l'établissement du contexte ISO 27005. Ces normes exigent que chaque organisation attribue un niveau de sensibilité et de criticité aux actifs afin d'assurer une protection adéquate au risque qu'elles sont exposées

Les actifs ont été catégorisé en plusieurs catégorie différente (Confidentiel, Employé, application, composante physique, concept, bâtiment et autres) soit actif primaire principal et actif de support. Ensuite, chaque actif a été évaluer selon leurs impacts sur la CIA.

Pour chaque pilier de la CIA, les actifs ont été évalué sur une échelle qualitative a 3 niveaux (1 étant faible et 3 étant élevé). Cette évaluation a été basé sur les analyses de l'actif au niveau des opération, son importance pour les processus, les obligations légales et normative, ainsi que son lien avec les services offert par l'organisation.

À partir de ces évaluations, un niveau de Criticité globale a été attribué à chaque actif. Pour voir la listes complètes des actifs avec le détail CIA et leur Criticité, vous référer à *l'annexe 1*

Méthode pour classifier, Type d'actif, Catégorie, actif, Propriétaire et dépendance, valeur, sensibilité, impact opérationnel, exigences légales.

Cette section représente une base pour l'analyse des risque (Section 9)

Section 9 — Analyse des risques

9.1 - Introduction à l'analyse du risque

L'analyse du risque est l'étape suivante après l'établissement du contexte. Afin d'évaluer les risques, l'utilisation d'ISO 27005 : 2022 a été appliquée afin d'analyser les actifs, les scénarios de menaces potentiel, ainsi que des vulnérabilités potentiels et l'impact qu'aurait une telle défaillance. Nous procéderons avec une technique d'analyse du risque basées sur les conséquences. L'utilisation de la méthode qualitative sera utilisée.

[2]Le but sera d'identifier les conséquences résultant de l'incapacité à préserver de manière adéquate la confidentialité, l'intégrité ou la disponibilité des informations.

Le processus d'identification des risques visera donc à décrire et analyser les risques (comprendre les types de risque et déterminé le niveau de risque). Le but ultime reviendra ensuite à une priorisation du risques critique et de se préparer aux différentes mesures de traitement (Section 10) et sélection des contrôles (Section 11).

Afin de mieux comprendre le risque, voir dans l'Annexe Définitions pour les définitions des actifs, du risque et des vulnérabilités.

L'identification du risque consiste en 3 étapes :

9.1.1 - Identification des risques

[12]L'identification des risques est la première étape. C'est un processus par lequel on reconnait et décrit tout risque qui pourrait impacter de façon négative l'organisation et les systèmes d'informations. Ces risques peuvent être identifier par des menaces techniques, physiques, humaines, processus métier, légales et réglementaire. L'analyse documentaire, les entretiens, les questionnaires, brainstorming, analyses de scénarios, modélisation des menaces, l'évaluation de vulnérabilité et l'utilisation d'outils logiciels sont des éléments pertinents afin d'identifier correctement le risque.

9.1.2 - Analyse et évaluation des risques

[12] L'évaluation doit se baser sur des critères prédéfinis. Un fois que le risque a bien été identifié, on doit procéder à l'évaluation du risque. C'est à dire de connaitre la potentialité de la survenance du risque ainsi que l'impact qu'il pourrait avoir sur l'organisation. Cette étape permet, entre autres, d'en déterminer la criticité et permet d'attribuer un indicateur de priorisation. L'évaluation de

l'impact peut être utilisé de façon qualitative ou quantitatif. L'évaluation de probabilité permet d'estimer la fréquence à laquelle un risque pourrait arriver ainsi que l'assignation du niveau de risque qui permet de combiner l'impact et la probabilité pour classifier le niveau du risque (faible, moyen, élevé, critique).

9.2 - Légende de niveau de criticité :

Voir l'annexe légende de niveau de criticité.

9.3 - Matrice d'exposition du risque:

Afin d'évaluer l'impact nous avons par la suite inséré une matrice d'exposition afin d'établir un barème claire identifiable sur l'évaluation du risque. La matrice d'exposition du risque est l'outil visuel qui servira de référence. Pour notre matrice d'exposition du risque vous pouvez vous référer à l'Annexe II.

9.4 - Matrice des risques selon ISO 27005:2022

Afin de bien identifier chaque risque, nous avons insérer pour chaque actif des scénarios identifiant des menaces et les conséquences associées. Ce tableau prend donc en considération (actifs, menace, vulnérabilité, probabilités, impact, conséquence) Ce tableau permettra entre autres de prioriser les risques critiques. Pour notre matrice de risque vous pouvez vous référer à l'*Annexe III.*

9.5 - Synthèse:

En résumé, notre approche qualitative repose sur des scénarios de conséquences. L'objectif étant d'identifier les risques, analyser leur niveau et d'évaluer le risque. L'impact est directement relié à la CIA (confidentialité, intégrité et disponibilité). Par la suite, quelques définitions tel que les vulnérabilités (technique, humaines et organisationnelle), la définition du risque (probabilité x impact) facilitent à la compréhension du risque. La structure des matrices est donc présentée en soutient au tableau de matrice des risque ISO 27005. Cette dernière démontre des menaces et des vulnérabilité (technique, humain et organisationnel).

Cette analyse fournit une base pour le traitement du risque (Section 10) et de la sélection des contrôles (Section 11).

Section 10 — Traitement des risques

10.1 Analyse préliminaire du traitement du risque

Le traitement du risque est l'étape suivante après l'identification, l'analyse et l'évaluation du risque. Une fois ces étapes complétées, si l'évaluation du risque est jugée conforme et que l'analyse est considérée acceptable avec une appréciation satisfaisante pour poursuivre le processus de gestion du risque, le traitement du risque est enclenché. Afin de traiter le risque, l'utilisation ISO 27005:2022 a été utilisée afin d'appliquer les concepts du traitement du risque (acceptation, mitigation, transfert, évitement).

Le traitement du risque doit se faire par ordre de priorité en fonction des critères de risque. Une fois les moyens mis en œuvre, le plan de traitement du risque permettra de modifier le risque pour qu'il réponde aux critères d'acceptation. Chaque décision devra être documentée principalement

pour la prochaine étapes (Section 11 - Sélection des contrôles) qui en aura besoin pour sélectionner les contrôles pertinents ainsi que pour les déclarations d'applicabilité.

10.2 - Sélection du traitement

La sélection du traitement du risques est importante, car elle aura un impact sur l'avenir de l'organisation. Il en donc prioritaire de sélectionner des traitements appropriés.

10.2.1 - Évitement

[12] Choisir d'éviter le risque en ne procédant pas à l'activité qui le génère. Évitement peut impliquer de changer des plans d'affaires ou de refuser des projets à haut risque.

10.2.1 - Mitigation (réduction)

[12] Prendre des mesures pour réduire la probabilité d'occurrence d'un risque ou en minimiser l'impact. La mise en place de contrôles supplémentaires ou le renforcement des contrôles existants sont des exemples de mitigation.

10.2.1 - Transfert

[12] Déplacer la responsabilité et l'impact financier d'un risque à une tierce partie, généralement par l'assurance ou des contrats. Le transfert est souvent utilisé pour les risques qui peuvent être couverts par des polices d'assurance ou d'autres arrangements contractuels.

10.2.1 - Acceptation

[12]Reconnaissance qu'un risque est acceptable sans action supplémentaire en raison de sa faible priorité ou coût de traitement élevé. Souvent utilisée pour les risques à faible impact et faible probabilité.

10.3 - Synthèse

En récapitulatif, le traitement du risque est la suite de l'identification, l'analyse et l'évaluation du risque. Lorsque jugée acceptable de continuer le processus, l'étape suivante est le traitement du risque. Pour donner suite à cela, quatre étapes sont utilisées : l'évitement, la mitigation, le transfert et l'acceptation. Le traitement est priorisé selon les critères de risques (voir Section 9 – Analyse des risques). Chaque décision doit être documenté.

Cette analyse fournit une base pour la sélection des contrôles (Section 11) qui introduira implicitement la continuité du traitement.

Section 11 — Sélection des contrôles

À la suite de la sélection du traitement du risque, tel qu'indiqué dans la section 10 du présent document, c'est à ce moment qu'on décide du choix des contrôles nécessaires afin d'éviter, réduire, transférer le risque et/ou le rendre acceptable.

11.1 - Analyse préliminaire de la sélection des contrôles

Popcorn communication choisie ses contrôles en fonction du traitement du risque choisi. Il se réfère à la section 6.1.3 de son guide normatif ISO 27001 :2022 combinés à ISO 27005:2022 sections 8 sur le processus de traitement du risque lié à la sécurité de l'information. L'entreprise détermine donc les mesures de sécurité qui sont nécessaires au traitement du risque choisi précédemment.

Elle documente la déclaration d'applicabilité en déterminant les contrôles nécessaires à l'application du traitement du risque. Une justification pour toute exclusion est requise et doit être pertinente. Toute exclusion ne doit pas faire référence à des élément critique pour la confidentialité, l'intégrité et la disponibilité et ne peut être admise que si le niveau de risque associé est faible. La déclaration d'applicabilité devra être cohérente entre les moyens de maitrise nécessaire et la réalisation des options des traitements du risque qui ont été sélectionné. Le statut de la mise en œuvre pourra être déclarée comme « mise en œuvre », « partiellement en œuvre » ou « non mise en œuvre ».

11.2- Choix du contrôle

Pour une vision plus claire sur notre sélection des contrôles choisis et du mapping ISO/NIST/CIS, vous référez à l'annexe V.

11.3 - Risque résiduels

Dans nos critères de sélection des contrôles, nous nous assurons que les risques résiduels soient acceptables. Cela correspond à une probabilité ajustée à la baisse et/ou une diminution des impacts afin qu'il nous reste que des risques résiduels faibles ou acceptables. Comme mentionné dans notre guide normatif, la direction doit accepter le risque résiduel restant sans quoi nous considérons les contrôles choisis insuffisants ou inadéquats.

Section 12 — Directives de sécurité

Les directives de sécurité définissent les règles opérationnelles permettant d'assurer la protection des actifs informationnels. Elles visent à appliquer correctement les principes fondamentaux de la sécurité de l'information, tels que la confidentialité, l'intégrité et la disponibilité. Elles soutiennent l'application des normes et cadres de références adoptés par l'entreprise, notamment l'ISO 27001:2022, ISO 27002:2022, ISO 27005:2022, les cadres NIST, ainsi que la loi 25. Elles s'appliquent à tous les employés, fournisseurs, partenaires et à toute personne ayant un accès au système d'information de l'organisation.

12.1 Contrôle d'accès et authentifications

L'objectif de cette directive est d'assurer que seuls les utilisateurs autorisés peuvent accéder aux systèmes, aux informations aux applications de popcorn communication, en appliquant le principe du moindre privilège.

12.1.1 Exigence générale

Utiliser une MFA pour tous les systèmes critiques, notamment Active Directory, les VPN, le SIEM, les bases de données et les API. Appliquer le principe du moindre privilège : les employés ne doivent avoir accès qu'aux données et systèmes strictement nécessaires à leurs fonctions. Examinez et révoquez régulièrement les droits d'accès des employés qui changent de poste ou quittent l'entreprise. L'intégration LDAP doit être gérée de manière sécurisée pour un contrôle d'accès

centralisé. Mettre en œuvre des mots de passe forts et uniques pour tous les systèmes et comptes. Exiger des changements réguliers de mots de passe ainsi qu'un niveau mot de passe de complexité élevé.

12.1.2 Gestion des identifiants

Chaque utilisateur doit disposer d'un identifiant unique dans Active Directory. Les comptes partagés sont interdits à l'exception des comptes de services. Les comptes inactifs doivent être désactivés dès qu'un employé quitte l'entreprise ainsi que lors d'absences prolongées.

12.1.3 Compte à privilèges

Les accès administrateurs doivent avoir une justification qui a préalablement été validé par le CISO. Les actions réalisées par les comptes à privilèges doivent être journalisées et surveillées par l'analyste SOC et le SIEM.

12.1.4 Cycle des accès

Dès l'embauche, la création des accès, en fonction du rôle. doit être approuvé par la direction des ressources humaines (DRH) et validé par le CISO. Pendant la durée de l'emploi, toute modification ou ajout de privilège doit être justifiée selon les besoins opérationnelles. Au départ de l'employé, la révocation complète des accès doit être effectuée dans les plus brefs délais. Les fournisseurs doivent avoir des accès temporaires ou limités.

12.2 Sécurité des postes de travail et équipements mobiles

Ces directives couvrent tous les postes de travail, les serveurs ainsi que tous les autres équipements de travail tel que les pda, téléphones, tablettes et ordinateurs portables.

12.2.1 Configuration de sécurité

Les postes de travail et les serveurs doivent obligatoirement respecter une configuration sécurisé conforme aux bonnes pratiques d'ISO 27002. Tous les appareils doivent être équipé d'un antivirus et être gardés à jour. Les mises à jour de sécurité doivent respecter le calendrier établi par la direction des technologies de l'information (DTI.)

12.2.2 Sécurité physique et logique

Les sessions doivent se fermées après 30 minutes d'inactivités. Tous les disques durs doivent être chiffrés.

12.2.3 Équipement des employés et techniciens

Telnet est interdit pour les techniciens. Cependant ils peuvent utiliser des protocoles sécurisés comme SSH, HTTPS et TLS. Les pda doivent être gérés par une plateforme qui gère les appareils mobiles et toute connexion externe doit passer par le VPN de l'entreprise

12.3 Sécurité des réseaux et des communications

12.3.1 Architecture et segmentation

Le réseau doit obligatoirement être segmenté en VLAN, en zone DMZ, EN réseau interne et zones d'administration ainsi qu'en réseau invité. Chaque environnement, tel que l'environnement de production, l'environnement de test ainsi que l'environnement de développement doivent absolument être séparé.

12.3.2 Firewall, ids, ips et surveillance

Toutes les données doivent être filtrées par les pares-feux Fortinet. Toute activité suspecte doit être analysée par le SIEM Splunk ainsi que Cisco Secure IPS. Tous les journaux doivent être conservés selon la procédure 13.5 de ce document.

12.3.3 Vpn

Toutes les connexions externes doivent se faire obligatoirement via le VPN. L'authentification multifacteur (MFA) est obligatoire pour tout accès au VPN.

12.3.4 Chiffrement des communications

Toutes communications ayant des données sensibles ou critiques doivent être chiffrées. Les certificats TLS doivent toujours être surveillés, renouvelés et gérés.

12.4 Classification et protection des données

12.4.1 Classification

Les données doivent être traitées selon leur niveau de classification définit dans l'inventaire des actifs et selon la triade CIA.

12.4.2 Données personnelles

Toute collecte de données personnelles doit être minimale et justifiée. Les données personnelles doivent être protégées par chiffrement, des contrôles d'accès appropriés et une journalisation adéquate. Toute fuite de données ou information doit être communiqué dans un délai maximal d'une heure pour la direction et de 72 heures à la clientèle.

12.4.3 Transfert et stockage

Toute donnée sensible doit être sauvegardée dans des systèmes approuvés. Tous les transferts vers des partenaires ou des tiers doivent être chiffrés et correctement encadré.

12.5 Sauvegarde et restauration

12.5.1 règle du 3-2-1

Popcorn communication applique cette règle : 3 copies des données. 2 supports diffèrent. 1 copie hors site pour la sauvegarde.

12.5.2 Exécution et contrôle

Toute sauvegarde doit être chiffrée. Des tests de restauration doit être effectués régulièrement. Les résultats des tests doivent être documentés et validé par le CISO.

12.6 DevSecOps

12.6.1 Cycle sécurisé

Le développement du logiciel de popcorn communication doit absolument intégrer la philosophie DevSecOps. Le code doit être revue et analysé.

12.6.2 Séparation des environnements

Aucune donnée réelle ne doit être utilisée pour les tests. Les déploiements en production doivent être approuvé par le CISO et la direction des technologies de l'information (DTI).

12.7 Sensibilisations

12.7.1 Formation

Une formation obligatoire doit être offerte tous les deux ans et il doit inclure du contenu sur le phishing, les mots de passes, la confidentialité et sécurité mobile.

12.7.2 Hygiène

Verrouiller son poste lors des absences, jamais partager les mots de passe, signaler immédiatement toute activité suspecte.

12.8 Supervision conformité et amélioration continue

12.8.1 Surveillance

L'analyse SOC surveille 24 heures sur 24 les évènements via Splunk, IDS et IPS ainsi que les antivirus et les journaux.

12.8.2 Audits

Les audits internes et externes réguliers assurent la conformité aux normes et lois.

12.8.3 Risque Résiduel

Les risques résiduels doivent être approuvé par la direction.

Section 13 — Procédures

13.1 Gestion des accès

L'objectif de cette procédure permet de créer, modifier ou supprimer un accès d'utilisateur. Cette procédure permet également de réduire les risques liés aux accès non autorisés ou obsolètes.

Pour les responsables de la procédure, le champ d'application et les étapes veuillez-vous référer à l'annexe XII.1

13.2 Sauvegarde et restauration

L'objectif de cette procédure permet d'assurer la protection, l'intégrité et la disponibilité des données au moyen de sauvegardes et de processus de restauration.

Pour les responsables de la procédure, le champ d'application et les étapes veuillez-vous référer à l'annexe XII.2

13.3 Gestion des incidents

L'objectif de cette procédure est de détecter, analyser, contenir et résoudre les incidents de sécurité et logs.

Pour les responsables de la procédure, le champ d'application et les étapes veuillez-vous référer à l'annexe XII.3

13.4 Gestion des changements

L'objectif de cette procédure est de s'assurer que tout changement est Analysé, documenté, testé et approuvé afin de réduire les risques (Dev, Test, Prod).

Pour les responsables de la procédure, le champ d'application et les étapes veuillez-vous référer à l'annexe XII.4

13.5 Gestion des journaux et de la journalisation

L'objectif de cette procédure est d'assurer la conservation et l'analyse des journaux permettant la détection d'incidents

Pour les responsables de la procédure, le champ d'application et les étapes veuillez-vous référer à l'annexe XII.5

Section 14 — Standards

14.1 Standard de mots de passe

L'objectif de ce standard consiste à définir les exigences minimales pour les mots de passe afin d'assurer une protection adéquate des comptes.

Champ d'application: Tous les employés, consultant, partenaire et clients

Exigences:

1. Longueur minimale de 12 charactères
2. Complexité obligatoire (Majuscules, minuscules, chiffre et symboles)
3. Réutilisation des mots de passe interdit avec une historique de 3 mots de passe
4. Expiration 60 jours
5. MFA obligatoire pour tous
6. Verrouillage après 3 tentatives échoué

Références: ISO 27002 8.5

14.2 Standard d'accès

L'objectif de ce standard est d'établir les règles de gestion des accès au systèmes et aux données

Champ d'application: Tous les système, Comptes utilisateur et comptes à privilège élevée

Exigences:

1. Le principe du moindre privilège doit être appliqué
2. La séparation des tâches doit être effectué afin de limiter les permissions supplémentaires.
3. Revue d'accès fréquent pour les comptes sensibles
4. La création des rôles doit être effectué par le DRH et le CISO
5. Les accès sont révoqués dès le départ de l'employé
6. Les accès des fournisseurs doivent être limité

Référence: ISO 27002 8.3 et 8.2

14.3 Standard de sauvegarde

L'objectif de cette politique vise à garantir la disponibilité, l'intégrité et la récupération en cas d'incidents

Champ d'application: Serveur, Bases de données, AD et autres

Exigences:

1. Les sauvegardes doivent être effectués quotidiennement
2. Les sauvegardes doivent être chiffré
3. Le Stockage doit être effectué avec la méthode 3-2-1 (3 sauvegardes, 2 diffèrent et 1 off site)
4. Les sauvegardes doivent être en rétention pendant 60 jours avant d'être archivé
5. Un test de restauration doit être effectué régulièrement
6. Accès aux sauvegardes doivent être limité
7. Vérification de l'intégrité des sauvegardes automatique

Référence: ISO 27002 8.13

Section 15 — Plan de communication

Le plan de communication de la PSI sert à assurer la compréhension, l'adoption et l'application correcte des exigences de sécurité pour Popcorn Communication. Il renforce la structure organisationnelle, réduit les risques humain et soutien la conformité aux normes ISO 27001, ISO 27002 et aux obligations légales de la loi 25. Le plan suit les exigences de la clause A.7.4 (Communication) de la norme ISO 27001:2022

[4]L'organisation doit déterminer les besoins de communication interne et externe pertinents pour le Système de management de la sécurité de l'information, et notamment :

15.1 Sujet à communiquer

- Mise a jours de la PSI et des directives ainsi que les procédures

- rôles et responsabilité en matière de sécurité

- formations et activités de sensibilisation sur le phishing, mot de passe et la confidentialité

- Rappel sur les bonnes pratiques et les nouveaux contrôles technologique du moment comme le MFA, VPN, antivirus

- Avis de sécurité urgent comme des cas d'incident ou de brèches confirmés

- Exigences et les obligations légale avec les fournisseurs

15.2 Quand communiquer

- Annonce a chaque année de la PSI et quand il y a une mise à jour importante

- Bulletin a chaque mois sur la sensibilisation ainsi que les bonnes pratiques

- Formations obligatoire à chaque deux ans pour la sécurité de l'information

- Communication urgente dans un délai d'une heure maximum pour les cas d'incident critique confirmé et 72h pour les brèches des données personnelles des clients

- rapport a chaque trois mois sur la sécurité et les incidents observer en interne

15.3 Avec qui communiquer

- Interne : Tous les employés comme les techniciens, RH, TI et la direction

- Externe : client, fournisseur partenaires technologique et les organismes réglementaire ainsi que les consultants

- Situation de crise : communication avec les relations publique et la direction

15.4 Comment communiquer

- Canaux internes : intranet, courriel, réunion d'équipe

- Canaux externe : courriels officiels aux clients ainsi que le site web

- Incidents : procédure de communication formelle qui inclus des messages préapprouves et l'approbation CISO et le CEO ainsi que la journalisation des avis

Section 16 — Gestion des incidents

16.1 Objectif

La gestion des incidents vise à établir un cadre fixe permettant de détecter, analyser, contenir, résoudre et effectuer une documentation efficace des incidents affectant la CIA ou les actifs informationnel.

16.2 Champ d'application

Cette politique s'applique à tous les employés, les applications, les systèmes, le réseau et les données gérés par Popcorn Télécom.

16.3 définitions

Incidents de sécurité: Tout évènement qui a un impact sur la sécurité de l'information.

Événement: Activité hors du commun qui n'a pas encore été confirmée comme incidents.

Alerte: Notification généré par un système de détection tel que le SIEM, un antivirus, un IDS ou un IPS.

16.4 Rôle et responsabilités

CISO/ISM: Responsable du processus global de la gestion des incidents.

Équipe SOC: Détection, triage et analyse.

DTI: Responsable de l'ensemble de l'infrastructure informatique et des sauvegardes.

DRH: Responsable des incidents si un employé est impliqué.

Employé: Doit signaler tout incident ou activité suspecte

16.5 classifications des incidents

La classification des incidents est basée sur 4 niveaux de Mineur à Critique. Pour plus d'information sur la classification du risque, veuillez-vous référer à l'annexe X.

16.6 Processus de la gestion des incidents

Le processus de la gestion des incidents de l'entreprise est basé sur les fonctions du NIST CSF 2.0.

16.6.1 Detect

L'objectif est de détecter rapidement les activités suspectes ou anormales et d'identifier les incidents potentiel afin d'évaluer l'impact.

Catégorie d'indentification:

- DE.AE: Analyse des événements suspect
- DE.CM: Surveillance en continue

Actions utilisées:

- Détection via SIEM, IPS et IDS
- Collecte des journaux
- Analyse Initiale
- Classification selon le niveau d'impact

16.6.2 Respond

L'objectif de cette phase est de répondre de façon efficace afin de l'imiter l'impact et protéger les actifs

Catégorie d'identification:

- RS.AN: Analyser l'incident
- RS.MA: Gestion de l'incidents
- RS.CO: Réponse à l'incident et communication
- RS.MI: Mitigation de l'incidents

Actions utilisées:

- Isolé le système compromis
- Bloquer le compte corrompu
- Bloquer le flux de données
- Appliquer les correctifs ou une contre mesure
- Obligations légales (Loi 25 si l'incident est relié à une fuite de donnée)

16.6.3 Recover

L'objectif de cette phase consiste à restaurer les services et renforcer les défense suites à un indicent.

Catégorie d’identification:

- RC.RP: Exécution du plan de restauration
- RC.RO: Communication à la suite de la restauration

Actions Utilisées:

- Restauration des données à partir de sauvegarde
- Remise en fonctions des systèmes
- Surveillance renforcée
- Analyse après incidents
- Mise à jour des contrôles, mesures de sécurité et de politique

Ref: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

16.7 Communication et escalade

- Les incidents de niveau 2 et plus doivent être signalé au CISO/ISM
- Les incidents de niveau 3 et 4 doivent être communiquer à la partie prenante
- Les fuites de données personnelles doivent être rapporté selon la l*oi 25*

16.8 Documentation

Chaque incident doit être inscrit dans le registre des incidents et inclure:

- Description détaillée de l’incidents
- Quel est l’impact
- Quelles actions ont été utiliser pour contenir, éradiquer ou mitiger l’incident
- Logs ou autre chose démontrant une preuve d’incident
- Recommandation

16.9 améliorations en continuent

Il est important d’effectuer un rapport poste incident pour tous les incidents supérieurs au niveau 2. Par la suite, une révision de l’évènement doit être fait afin de s’assurer que celle-ci ne sera pas reproduite.

Section 17 — Plan de continuité

17.1 Objectif

Le plan de continuité vise à assurer la continuité des opérations de l’organisation en cas d’interruption. Il s'appuie sur les principes du NIST CSF et sur les bonnes pratiques de la continuité d’affaires.

17.2 Champ d’application

Ce plan couvre toute actifs primaire principal et actifs et support :

- Processus d’affaire et activités de l’entreprise et Informations
- Matériel, logiciel, réseau, personnel, site et structure de l’organisation

17.3 Rôles et responsabilité

- CEO: Déclenche le plan et approuve les ressources requises
- CISO/ISM: Coordonne la reprise et évalue les risques et l'impact
- DTI: Exécute les actions de restauration et redémarre les systèmes selon le niveau de priorité
- DRH: Effectue la communication avec les employées et communication externe au besoin
- DFO: Évalue l'impact financer et autorise les dépenses

17.4 Catégorisation et niveau de priorité

Les systèmes sont classés selon leur niveau de criticité sur un échelle de 1 à 3. Pour plus d'informations ou des exemples, veuillez-vous référer à l'annexe XI.

17.5 Sinistre couverts

Le plan couvre les interruptions suivantes:

- Cyberattaque
- Panne de courant
- Bris matérielle (Serveur, stockage, etc…)
- Indisponibilité du site web
- Perte de données

17.6 Stratégie pour la continuité

17.6.1 Sauvegardes

- Sauvegarde quotidienne avec option hors site (Méthode 3-2-1)
- Sauvegarde chiffrée
- Test de restauration

17.6.2 Redondance

- Virtualisation pour une reprise rapide
- Redondance réseau
- Environnements séparés pour les applications critique

17.7 Processus de reprise

1. Activation du PRA (plan de reprise d'activité) par la direction
2. Utilisation de ressources de secours (Si applicable)
3. Restauration des systèmes critique et validation de l'intégrité des systèmes
4. Restaurations des systèmes non critique
5. Test de fonctionnalité
6. Logs et documentation

17.8 Test du plan

Afin d'assurer l'efficacité du plan, il est important de le tester sous plusieurs niveaux, incluant le table top, le test partiel et le test complet. L'organisation se doit d'effectuer des tests réguliers selon les bonnes pratiques des normes ISO ou du NIST CSF.

Objectif des tests:

- Assurer le bon fonctionnement du plan de reprise
- Identifier de potentiel problème
- S'assurer que tous les employés effectuent leur rôle correctement
- Valider l'intégrité après une restauration

Il est important que chaque test soit documenté afin d'analyser les problèmes et les corrigés.

17.9 Mise à jour et révision

Le plan de continuité doit être révisé régulièrement afin de refléter l'évolution technologique, organisationnelle et réglementaire.

Fréquence de révision:

- Une révision complète doit être effectuée annuellement.
- Le plan doit être revue après chaque incident majeur
- Après chaque teste significatif si un correctif a été appliqué
- Lors d'un gros changement de logiciel ou d'infrastructure

Contenu a révisé:

- Classification des systèmes
- Délais RTO et PRO
- Procédure de restauration
- Plan de communication
- Processus d'amélioration en continue

Chaque révision doit:

- Être datée
- Approuvée
- Documenté

Section 18 — Gestion documentaire, mise en vigueur, révision

18.1 - Introduction à la gestion documentaire

Cette présente politique relève directement du CEO (Chef de la direction), mais est directement modifié par le RSSI (CISO dans notre cas). Cette dernière doit être comme une entité à part entière et doit être réviser minimalement de façon annuelle. Chaque changement doit être inscrit dans cette section afin de garder une traçabilité afin que ce document ne représente pas une entité statique, mais plutôt dynamique. Elle doit aussi servir aux fins d'audit interne ou externe et spécialement dans un contexte de validation de conformité des normes et de certification.

18.2 - Information complémentaire et mise en vigueur

Numéro de version du document : 0.0.1

Date de création du document : 1er décembre 2025

Mise en vigueur : 14 décembre 2025 - *Date d'approbation du CEO

Auteur : Chloé Arsenault, Janie Sarrazin, César Escobar Garcia, Émilien Gagnon et Simon-Pierre

18.3 - Fréquence et révision

Historique de modifications. Tout changement doit être indiqué ici:

Version	Date	Auteur	Validation	Modification
0.0.1	14 décembre 2025	RSSI (CISO)	CEO	Initialisation du document

Références normatives : * Voir l'annexe Référence *

Fréquence de révisions : Minimalement annuelle

Processus de Mise à jour : Suivant la fréquence recommandée, le RSSI, dans ce cas-ci le CISO se doit d'enclencher de processus de validation et mise à jour de cette présente PSSI. Il se doit de la maintenir conformes aux normes et loi en vigueur dans la province, dans le pays, et du respect des normes suite ISO, NIST et CSC.

Section 19 — Conclusion stratégique

19.1 - Synthèse global

En conclusion, un rappel des différentes stratégies implémenté tout au long de l'intégration de cette PSSI. Elle vise à la représentation des normes d'application et légal.

Enjeux informationnels

Pour commencer l'entreprise énonces les enjeux informationnels lié à la confidentialité, l'intégrité et la disponibilité ainsi que tout ce qui a trait à la traçabilité, réputation, enjeux liés à l'économie et à tout ce qui est conformité légale et réglementaire. Elle fait notamment référence à l'ISO 27001:2022 pour la clause 4 contexte de l'organisation, clause 5 Leadership

Champ d'application de la politique

Par conséquent, une cartographie du champ d'application de cette politique a été implémenté aux personnes, actifs et activités afin d'appliqué la sécurité de la triade et la conformité légal tant provincial que fédéral. À nouveau ici nous utilisons l'ISO 27001:2022 qui s'aligne sur les conformités d'un SGSI aux clauses 4.3 sur la détermination du domaine d'application et la clause 5 pour le leadership.

Cadre légal et normatif

L'entreprise exprime par la suite une volonté de respecter les différents cadres légaux autant au niveau provincial que fédéral. Elle utilise à nouveau l'ISO 27001:2022 entre autres les clause 4 dans contexte de l'organisation et clause 5 leadership, clause 6 planification et 7 supports.

Principe de sécurité

Elle élabore des principes de sécurité afin de respecter non seulement le cadre légal, mais aussi d'instaurer un régime de sécurité au sein de l'entreprise. Le NIST CSF 2.0 SP-800-30, 53, 34 et

207 a été utiliser dans cette section afin de promouvoir les normes sur les opérations, réponse aux incidents, zéro trust, principe de défense en profondeur.

Gouvernance

Par la suite l'élaboration d'une gouvernance ainsi que le rôle de chacun de ces acteurs est définit ainsi que leurs responsabilités. L'utilisation d'ISO 27001:2022 clauses 5 Leadership et 7 supports sont notamment utilisé.

Inventaire et classification

S'en suit par l'établissement du contexte (ISO 27005:2022 articles 6). C'est à dire la définition du risque, de la vulnérabilité et de la potentialité et par la déclaration de l'inventaire global des actifs informationnels et de leur classification et de leur propriétaire dans l'entreprise.

Analyse des risques

Ensuite nous avons procédé par l'analyse des risques (ISO 27005:2022 articles 7.2, 7.3, 7.4). Dans cette optique, l'identification des risque, l'analyse du risque et l'évaluation du risque était au cœur de ce chapitre. L'utilisation de la méthode qualitative (faible, moyen, élevé, critique) basé sur l'identification de la criticité des scénarios de menace et sur la potentialité de conséquence possible sur la confidentialité, l'intégrité et la disponibilité. Un classement en ordre de priorité critique a donc été élaboré.

Stratégies de traitement du risque

Dans cet ordre, les stratégies de traitement sont la prochaine étape (ISO 27005:2022 articles 8). À la suite de l'évaluation conforme du risque et de l'analyse jugée acceptable et satisfaisante pour poursuivre l'application des 4 concept du traitement sont enclenché (Acceptation, mitigation, transfert et évitement) par ordre de priorité. Autrement dit, chaque risque doit être identifié et relié à une action de traitement dans l'ordre la plus prioritaire à traité. Chaque action est documentée et justifiée (ISO 27005:2022 articles 10.4). Cela assure la traçabilité.

Sélection des contrôles

Dans le cadre de la sélection des contrôles, tous les contrôles retenus afin de se protéger contre les risques sont identifiés. Ce cadre s'appuie sur ISO 27001:2022, ISO 27002:2022, NIST-800 53 et des contrôles CIS v7 afin de couvrir le plus large éventail, de renforcir les exigences. Le tout en ne se limitant pas à un seul choix.

Directive de sécurité

Les directives de sécurité définissent les règles pour protéger les actifs tant au niveau confidentialité, intégrité que disponibilité et veut s'assurer que la conformité des différentes normes et lois tant provincial que fédéral avec l'utilisation des différents documents ISO 27001:2022, 27002:2022, NIST et de la loi 25. Cette directive s'adresse à toute les employés, fournisseur et partenaires. Elle parle entre autres des contrôles d'accès et authentification, de la sécurité des postes de travail, sécurité réseau, de la protection des données, sauvegarde, de la sensibilisation, de la supervision, conformité et amélioration ainsi que de la philosophie DevSecOps engendrer tout aux longs des processus de développement.

Procédure

Elle démontre par la suite des procédures qui définissent les étapes à suivre pour assurer une gestion de la sécurité au sein de l'organisation. Par exemple au niveau de la gestion des accès utilisant les contrôles du ISO 27002:2002 8.2 et 8.3 ou encore au niveau de la sauvegarde et restauration en

utilisant les contrôles NIST 800-34. Chacune de cette procédure parle notamment du responsable, d'une association au différent champ d'application des contrôles, des étapes à suivre et de leurs références

Standards

Les standards essentiels appliqués servent à renforcir la sécurité et la conformité avec les bonnes pratiques. L'utilisation conforme d'ISO 27002:2022 a été utiliser afin d'avoir les meilleures pratiques de l'industrie. L'implémentation de standard tel que les standards de mot de passe offrant une robustesse des mots de passe, d'accès sécurisé et de sauvegarde fiable ; le tout garantissant la confidentialité, l'intégrité et la disponibilité des informations sont au cœur même de ce chapitre.

Plan de communication

Le plan de communication établie un cadre de communication qui sert à garantir la compréhension, l'adoption et l'application de toutes les exigences de sécurité servant à renforcir la structure de l'organisation en réduisant les risques et en appliquant une conformité aux normes ISO 27001:2022 en s'alignant sur les clauses A.7.4 Communication, 27002:2022 et aux différentes obligations légales provincial et fédéral tel que la loi 25. Il évoque le sujet à communiquer, quand le communiquer, avec qui le communiquer et comment le communiquer.

Processus de gestion des incidents

Le processus de gestion des incidents implémente les concepts de détection (DE.AE analyse des événement et DE.CM surveillance continue), réponse (RS.AN analyse, RS.MA gestion et RS.MI mitigation) et recouvrement (RC.RP plan de restauration, (RC.RO communication post-restauration) face à l'incident en s'alignant conformément aux normes du NIST CSF 2.0. Il garde les concepts de niveau d'escalade 1 à 4, de documentation et d'amélioration continue post-incident. Cela assure une traçabilité et conformité légal tout en renforçant la gestion de la sécurité de l'organisation.

Plan de continuité

Le plan de continuité qui vise au suivi aux opérations post-incident en cas d'interruption s'appuie lui aussi sur les bonnes pratiques sur le NIST CSF 2.0. Il parle du champ d'application, des rôles et responsabilités, catégorisation et criticité, des différents sinistres couverts, des stratégies de continuité, processus de reprise, plan de test et mise à jour et révision le tout intégrant entre autres la sauvegarde, la redondance et des audit régulières.

Gestion documentaire, mise en vigueur et révision

Pour finir nous avons la gestion documentaire qui vise à établir un plan de modifications dynamique pour cette présente PSSI visant à la conformité des normes ISO 27001:2022 et à l'amélioration continue. Elle confirme aussi la volonté de la direction au maintien de cette PSSI.

Annexe

Les différentes annexes serviront pour les référence interne dans cette PSSI.

19.2 - Récapitulation sur l'alignement stratégique

En conclusion l'utilisation des meilleures normes et standard internationaux incluent l'ISO, NIST et CIS. L'entreprise s'aligne aussi sur toute les normes provincial et fédéral. Le but étant de ne pas se limiter à un seul document de norme, mais bien de faire l'intégration des différents concepts,

normes et contrôles les plus maitriser et les plus convenable, sélectionner de façon méticuleuse pour l’entreprise et de respecter tout loi en vigueur s’appliquant à l’entreprise.

Section 20 — Annexes obligatoires

Annexe - Définitions

- AD – Active Directory
- **UI** – User Interface
- **IOT** – Internet Of Things
- **PME** – Petite et moyenne entreprise.
- **PDA** – Personal Digital Assistant
- **DNS** – Domain Name System
- **API** – Application Programming Interface
- **LDAP** – Lightweight Directory Access Protocol
- **SIEM** – Security Information and Event Management
- **SaaS** – Software As A Service
- **VPN** – Virtual Private Network
- **IDS** – Intrusion Detection System
- **IPS** – Intrusion Prevention system
- **VLAN** – Virtual Local Area Network
- **DMZ(DZ)**– Demilitarized zone
- **ERP** – Enterprise Resource Planning
- **RH** – Ressources humaine
- **VM** – Virtual Machine
- **GDPR** – General Data Protection Regulation
- **VOIP** – Voice Over Internet Protocol
- **TCP** – Transmission Control Protocol
- **HTTP** – Hypertext Transfer Protocol
- **SMTP** – Simple Mail Transfer Protocol
- **(C#, Angular, HTML, CSS)** - Programming language
- **Dotnet** – Microsoft OpenSource Framework
- **Intranet** – Local ou restreint réseau de communication
- **WWW** – World Wide Web
- **OnPrem** – In-House – Serveurs maison
- **TI** – Technicien Informatique
- **SGSI** – Politique de Sécurité des Système d'information
- **Telnet** – Protocol internet de connexion non sécurisé
- **SSH** – Secure Shell
- **SSL** – Secure Socket Layer
- **TLS** – Transport Layer Security
- **Actifs -** ISO 27005 Définit 2 types d'actifs dans un périmètre
  Actifs primaire/Principal :
  Processus d'affaire et activités de l'entreprise
  Informations
  Actif de support : Matériel, logiciel, réseau, personnel, site et structure de l'organisation

- **Vulnérabilité** -
  Technique : Vulnérabilités liées aux systèmes, logiciel, matériel ou configuration.
  Humain : Vulnérabilité liés aux comportement humain, erreurs ou manque de compétences humaine.
  Organisationnel : Vulnérabilités liées aux processus incorrecte, politiques, gouvernance et ou absence de planification.

- **Probabilité** - La **probabilité** c'est la chance qu'a l'attaquant a d'exploite une vulnérabilité (Très improbable, improbable, probable, très probable)
- **Impact** - **L'impact** c'est le résultat de l'exécution d'une menace (faible, moyen, élevé, critique)
- **Risque** - Le **risque** c'est la **Probabilité** x **l'impact**

Annexe I – Inventaire des actifs détaillés

* Classification selon ISO 27005
* Voir définition Actifs dans définition

	Actifs	**C/I/A**	**Classification**	**Criticité**	**Propriétaire**
Confidentiel (Actif/primaire)	Données clients	3/3/2	Très critique	Critique	CISO
	Données financières	3/3/2	Confidentiel	Élevée	CFO
	Données employées	3/3/2	Confidentiel	Élevée	DRH
	Information personnelles (loi25, GDPR)	3/3/2	Très critique	Critique	GRC
	Secrets industriels	3/3/1	Confidentiel	Élevée	CEO
	Propriété intellectuelle	3/3/2	Confidentiel	Élevée	CEO
	Logs de sécurité	3/3/3	Confidentiel	Critique	CISO/Soc
	Database	3/3/3	Très Critique	Critique	DBA/DTI
	Document internes	2/2/1	Interne	Moyenne	DG
	Dossier employé	3/3/2	Confidentiel	Élevée	DRH
	Dossier Client	3/3/3	Très critique	Critique	CRM
	Contrats	2/3/2	Confidentiel	Élevée	Responsable juridique

	Plans de projets	2/2/1	Interne	Moyenne	DTI
	Courriels	2/3/2	Confidentiel	Élevée	DTI/Infra/Support
	Backups	3/3/2	Très Critique	Critique	DTI/Infra
Employé (Actif de support)	Employés	2/2/2	Interne	Moyenne	DRH
	Direction	3/3/2	Confidentiel	Élevée	CEO
	DSI	3/3/3	Très critique	Critique	DTI
	Administrateur système	3/3/3	Très critique	Critique	DTI
	Partenaires externes				
	- Prestataires	2/3/2	Confidentiel	Élevée	DRH
	- Consultants	2/3/2	Confidentiel	Élevée	DRH
	Stagiaires	1/2/1	Interne	Faible	DRH
Software (Actif de support)	Système d'exploitation	2/3/3	Interne	Élevée	DTI
	ERP	3/3/2	Confidentiel	Élevée	DTI
	CRM	3/3/3	Très critique	Élevée	CFO
	Logiciel de comptabilité	3/3/2	Confidentiel	Élevée	CFO
	Antivirus (Norton) SIEM (Splunk)	3/3/3	Interne et très critique	Critique	CISO/Soc
	API (C#, Python, etc.)	3/3/3	Très critique		CISO/Dev
	Web/API (HTML, Angular, CSS...)	3/3/2	Confidentiel	Élevée	DTI/Dev
	Intranet (Angular)	2/2/2	Interne	Moyenne	DTI

	Système comptable	3/3/2	Confidentiel	Élevée	CFO
	Outils DevOps	3/3/2	Confidentiel	Élevée	DTI/DevOps
	Outils de sauvegarde	3/3/3	Très critique	Critique	DTI/Infra
	Script automatisé	2/3/2	Interne	Moyenne	DTI
	SaaS	3/3/3	Très critique	Critique	DTI
	Docker (Container; VM)	3/3/3	Très critique	Critique	DTI/Infra
	Firewall (Fortinet)	3/3/3	Très critique	Critique	CISO/Soc
	IDS/IPS (Cisco secure IPS)	3/3/3	Très critique	Critique	CISO/Soc
	VPN (Nord VPN)	3/3/3	Très critique	Critique	DTI//Infra
	Poste de travail	2/2/2	Interne	Moyenne	DTI/Support
	Bureau virtuel	3/3/3	Confidentiel	Élevée	DTI/Support
	DNS	3/3/3	Très critique	Critique	DTI /Infra
Hardwares (Actif de support)	Serveur	3/3/3	Très critique	Critique	DTI/Infra
	Router	2/3/3	Très critique	Critique	DTI /Infra
	Reverse Proxy	2/3/3	Confidentiel	Élevée	DTI/Infra
	Câblage	1/2/3	Interne	Élevée	DTI /Support
	PDA	2/2/2	Interne	Moyenne	DTI /Support
	Switch	2/3/3	Très critique	Critique	DTI/Infra
	Ordinateur portable	2/2/2	Interne	Moyenne	DTI /Support
	Ordinateur bureau	2/2/2	Interne	Moyenne	DTI /Support
	Téléphones	1/2/2	Interne	Moyenne	DTI /Support

	Tablettes	1/2/2	Interne	Moyenne	DTI/Support
	Imprimantes	1/2/1	Interne	Faible	DTI /Support
	Scanners	1/2/1	Interne	Faible	DTI/Support
	Disque dur externes	3/3/2	Confidentiel	Élevée	DTI /Infra
	Ondulateurs (UPS)	1/2/3	Confidentiel	Élevée	DTI /Infra
	Caméra de sécurité	2/2/3	Confidentiel	Élevée	DTI
Concept (Actif de support)	VLAN	2/3/3	Interne	Élevée	DTI /Infra
	DMZ	2/3/3	Confidentiel	Critique	DTI /Infra
	Réseau Interne	2/3/3	Confidentiels	Élevée	DTI /Infra
	LDAP	3/3/3	Très critique	Critique	DTI /Infra
	Réseau Wi-Fi	2/2/3	Interne	Élevée	DTI /Infra
	VPN	3/2/3	Confidentiel	Critique	DTI /Infra
	Connexion internet	1/3/3	Très critique	Critique	DTI /Infra
	Architecture réseau	3/3/3	Très Critique	Critique	DTI/Infra
Physique (Actif de support)	Bâtiment	1/2/3	Interne	Élevée	CISO/CEO
	Salle de serveurs	3/3/3	Très Critique	Critique	CISO/CEO
	Cabinets fermés à clé	2/3/3	Confidentiel	Critique	CISO/CEO
	Système d'alarme	2/2/3	Confidentiel	Élevée	CISO/CEO
	Climatisation	1/2/3	Interne	Élevée	CISO/CEO
Autres (Actif primaire)	Processus RH	3/3/3	Confidentiel	Élevée	DRH
	Processus d'accès	3/3/3	Très Critique	Critique	CISO
	Politique de sécurité (PSSI)	1/3/3	Public	Moyenne	DTI
	Procédure opérationnelle	2/3/2	Interne	Moyenne	CISO

	Procédures d'incidents	2/3/3	Confidentiel	Élevée	CISO
	Plan de continuité (BCP)	3/3/3	Très Critique	Critique	CISO
	Plan de reprise (DRP)	3/3/3	Très Critique	Critique	CISO
	Registre d'accès	3/3/3	Confidentiel	Élevée	CISO
	Gestion des correctifs	2/3/3	Confidentiel	Critique	DTI/CISO

Annexe II – Matrice d'exposition du risque

Risque x Probabilité	**Très improbable**	**Plutôt improbable**	**Plutôt probable**	**Très probable**
Non-significatif	Faible	Faible	Faible	Moyen
Important	Faible	Moyen	Moyen	Élevé
Grave	Moyen	Moyen	Élevé	Critique
Très grave	Élevé	Élevé	Critique	Critique

Annexe III – Matrice de risque

* Ordre de classement effectué selon niveau de risque du plus critique au risque le plus faible (prioritaire au moins prioritaire)

*Basé sur : valeur, sensibilité, impact opérationnel, exigences légales.

Actif	**Menace**	**Vulnérabilité (Technique/Humain/Organisationnel)**	**Impact (CIA)**	**Probabilité**	**Niveau de risque**	**Conséquence**	**Classement (ordre de priorité)**
Base de données clients	Intrusion externe	**Tech** : Mise à jour manquante **Hum**: Mot de passe faible **Org**: Aucune politique	Élevé	Élevé	Critique	Fuite de données et sanctions Loi 25 Perte de confiance.	1 (Exigence légal)

		de sécurité sur les mots de passe				Perte de crédibilité. Perte financière	
Serveur	DDOS (Mirai)	**Tech** : Manque de segmentation réseau **Hum** : Manque de formation et ou sensibilisation. **Org** : Manque de procédure pour contrôler l'attaque; Pas de plan de continuité	Élevé	Élevé	Critique	Potentialité de diversion pour attaque autre ex: Intrusion Interruption de service Retard dans les projets Dysfonctionnement technique	2
Active-Directory	Kerberoasting	**Tech** : Hash non sécurisé et ou mal configurer (Ex : RC4) **Hum**: Administrateur pas former aux bonne pratiques **Org**: Pas d'audit régulier	Élevé	Élevé	Critique	Intrusion dans les serveurs. Potentialité pour mouvement latéral. La CIA au complet est touchée ici	3
PDA	Attaque Man-In-The-Middle	**Tech** : Transfert non-sécurisé (FTP, HTTP) **Hum**: Manque de formation; Personnel se connecte sur réseau public	Élevé	Moyen	Élevé	Écoute sur le réseau;	10

		Org : Manque de responsable sécurité (Ex : CISO)				Fuite de données potentiel.	
Courriel	Phishing	**Tech** : Absence de détection d'intrusion (IDS/IPS) **Hum** : Click sur lien frauduleux : Manque de formation au phishing **Org** : Pas de formation aux employés dans les politiques de sécurité	Élevé	Élevé	Critique	Intrusion dans les systèmes. Potentialité de défaillance sur CIA au complet. Stress accrus Fraude ou vol	4
API Site web (Popcorn communication) et Database	Injection de dépendance	**Tech** : Application vulnérable à l'injection SQL **Hum**: Manque de connaissance sur le sujet d'injection **Org**: Pas de simulation de crise	Élevé	Moyen (Car système aujourd'hui sont généralement protégé)	Élevé	Fuite de données et sanctions Loi 25 (RGPD) Perte de confiance. Perte de crédibilité. Perte financière	6
Poste de travail (Windows)	Zero day (Example d'attaque:	**Tech** : Mise à jour Windows manquante **Hum**: Employé n'a pas fait la mise à jour, car en vacances.	Élevé	Moyen	Élevé	Intrusion dans les systèmes.	7

	Eternal Blue, Eternal Romance)	**Org**: Aucune volonté de remplacement d'employé durant les vacances				Potentialité de défaillance sur CIA au complet.	
Logs	Attaque non répertoriée	**Tech** : Mise en place de contrôle technique pour le log insufisant **Hum**: Manque de compétence sur SIEM(Soc) **Org**: Absence de procédure pour gérer des événements	Élevé	Moyen	Élevé	Non visibilité d'attaque (CIA menacé)	8
Employés	Ingénierie sociale	**Tech** : Action technique non autorisé tel que dévoilement d'information confidentiel **Hum**: Incapacité à détecter un comportement anormal **Org**: Absence de politique de sécurité	Élevé	Élevé	Critique	Fraude ou vol Stress accru Perte de confiances Poursuite judiciaire Augmentation des primes d'assurance	5
Contractant	Contractant ne suit pas les normes, politiques ou loi	**Tech** : Système du contractant non sécurisé **Hum**: Manque de sensibilisation sur les lois (Ex: Loi 25) **Org**: Contrat	Élevé	Moyen	Élevé	Fuite de données et sanctions Loi 25 (RGPD)	9

	en vigueur	fournisseur sans clause de sécurité				Perte de confiance. Perte de crédibilité. Perte financière	

Annexe IV – Registre d'autorité

Domaine de sécurité	**Autorité décisive**	**Autorité opérationnelle**	**Champ d'autorité**
Politique de sécurité (Doit être communiqué à tous les utilisateurs)	CEO	CISO/Analyste GRC	Le CEO approuve la politique et le GRC établie la PSSI.
Gestion du risque (Doit être communiqué à tous les employés)	CISO	Analyste GRC	Le CISO fait la mise en place stratégique GRC identifie, priorise et fait la mise en place
Réponse aux incidents de sécurité (Doit être communiqué ai CEO, DTI et GRC)	CISO	Analyste SOC	Le CISO dirige et supervise, l'analyste SOC détecté et collabore au rétablissement
Sécurité de Infrastructure/serveurs (Doit être communiqué au CISO/Analyte SOC)	DTI	Infrastructure	DTI approuve l'infrastructure et le responsable de l'infrastructure sécurise et s'assure de la redondance
Sécurité et segmentation réseau (Doit être communiqué au CISO/Analyste SOC)	DIT	Réseau	Le DTI gère et approuve l'ensemble du système et le responsable réseau surveille, analyse et segmente le réseau
Gestion des accès (Doit être communiqué aux CISO et aux Chefs des départements des employés)	DRH	Support TI	La direction des RH autorise l'attribution des accès et les TI gère les accès et renforcie l'authentification
Protection des renseignements personnels	CISO/DRH/LÉGAL	RH	Le CISO & la DRH doivent s'assurer que les mesures de protection

(Doit être communiqué à tous les utilisateurs et employés)			sont mises en place et respectés.
Développement sécurisé des applications (Doit être communiqué au CISO)	DTI	DevSecOps	DTI doit s'assurer et gérer la mise en place de mesures de protection et le DevSecOps revoit les codes et corrige les vulnérabilités/failles
Sécurité des postes de travail (Doit être communiqué au CISO)	DTI	TI	Le DTI est responsable des méthodologies et les TI sécurise les postes, applique les correctifs et mise à jour
Formation et sensibilisation (Doit être communiqué au CISO et à tous les employés)	DRH		S'assure d'une formation/sensibilisation envers la sécurité de l'information en continue
Signalement d'incidents (Doit être communiqué à tous les employés)	CISO	Analyste GRC	Le CISO impose les exigences et le l'analyste GRC doit mettre en place et assurer un suivi du registre des incidents

Réf : ISO 27001 :2022 5.3 *La direction doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.*

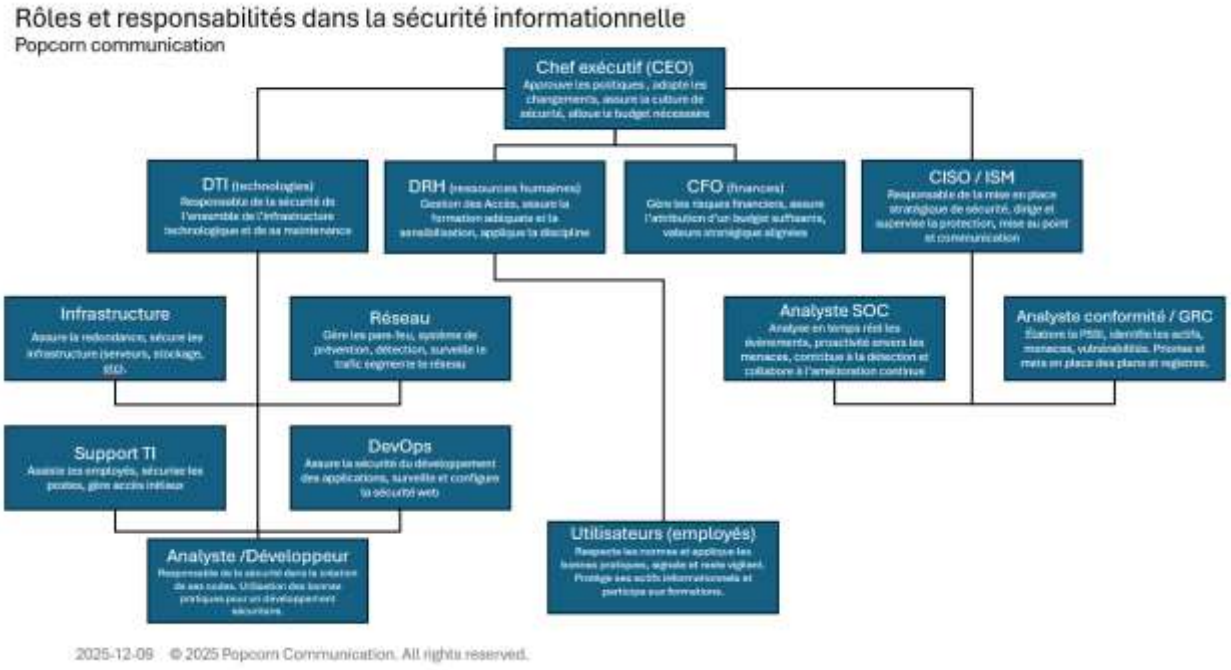
Annexe V – DDA et tableaux de mapping ISO/NIST/CIS

Élément	**Détail**		
Risque	Intrusion interne (fuite de la base de données clients via un accès non autorisé)		
Choix de traitement	Réduction du risque		
Contrôles sélectionnés	Iso27001 :2022 **A.5.15** Contrôle des accès	Nist-CSF 2.0 **PR-AA-01** *Gestion des identités, authentification et contrôle d'accès/01-gestion par l'organisation*	Cis Controls v7 **Cis-14** – *controlled access based on the need to know*

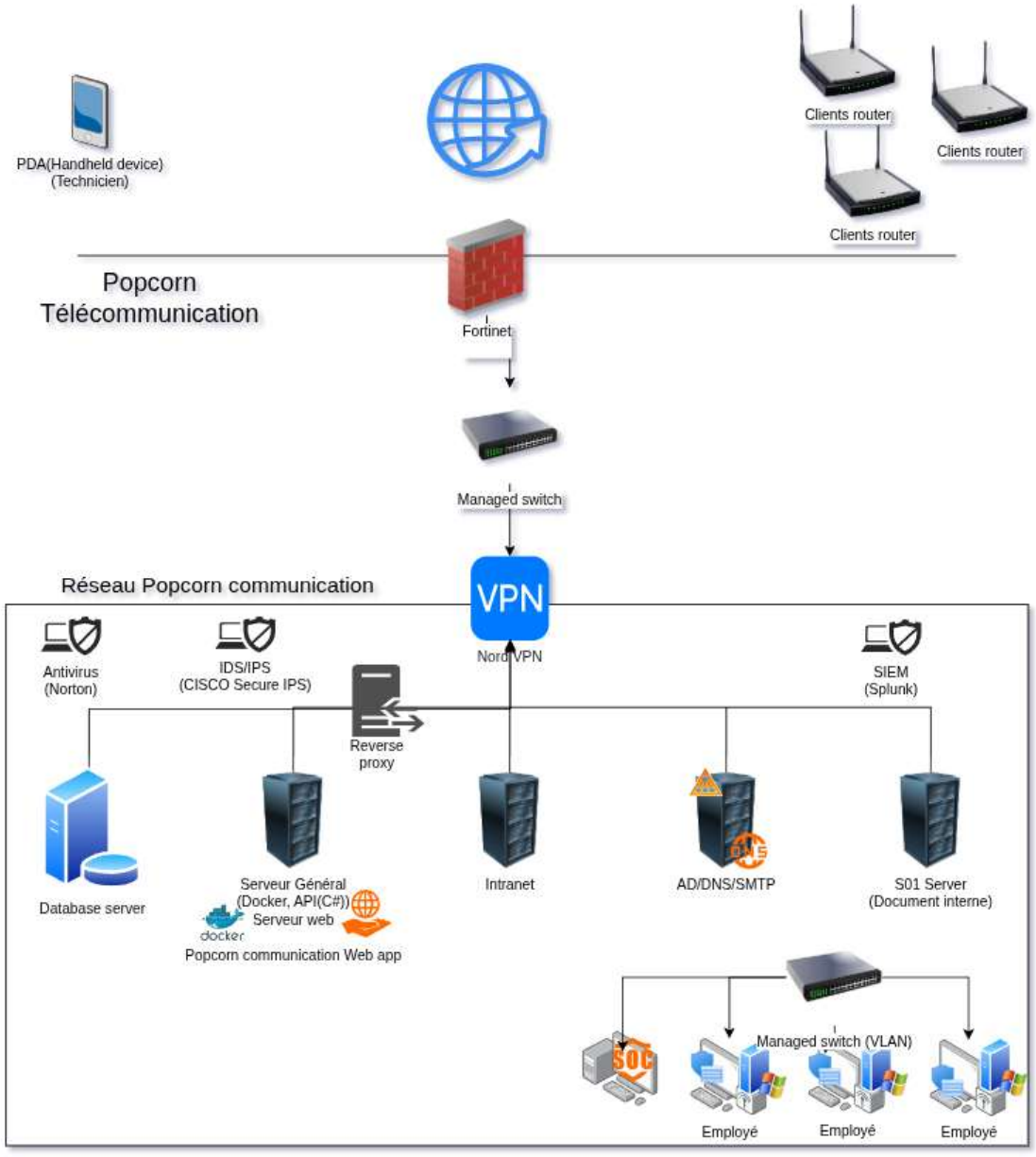
	A.8.5 authentification sécurisé (MFA)	**PR-AA-03** *(Gestion des identités, authentification et contrôle d'accès/03-utilisateurs, services et matériel authentifiés)*	**CIS-16** account monitoring and controlled
Justification	Ces contrôles diminueront les chances d'intrusions en rendant l'accès beaucoup plus difficile avec la gestion des comptes et l'authentification renforcée.		
Statut :	Mise en œuvre.		
Élément	**Détail**		
Risque	DDoS (interruption de service, tentative de diversion, etc.)		
Choix de traitement	Réduction du risque		
Contrôles sélectionnés	Iso27001 :2022	Nist-CSF 2.0	Cis Controls v7
	A.8.22 cloisonnement des réseaux	**PR.IR-01**résilience de l'infrastructure technologie / 01-réseaux et environnement protégés	**CIS-12** boundary défense
	A.8.21 sécurité des réseaux	**PR.IR-01** résilience de l'infrastructure technologie / 01-réseaux et environnement protégés)	**CIS-12** boundary défense
	A.8.16 activité de surveillance	**DE.CM-01** Surveillance en continue / 01-les réseaux et services réseaux sont surveillés	**CIS-6** maintenance monitoring
Justification	Ces contrôles aideront à contrôler ce qui entre et sort du réseau, détecter en analysant les journaux. En ajoutant le cloisonnement réseau et le dimensionnement, cela diminuera les chances d'une attaque réussie.		
Statut :	Mise en œuvre.		
Élément	**Détail**		
Risque	Kerberoasting (intrusion dans les serveurs)		
Choix de traitement	Réduction du risque		
Contrôles sélectionnés	Iso27001 :2022	Nist-CSF 2.0	Cis Controls v7
	A.8.22 cloisonnement des réseaux	**PR.IR-**01 résilience de l'infrastructure technologie / 01-réseaux et environnement protégés	**CIS-12** boundary Défense
	A.8.16 activité de surveillance	**DE.CM-01** (Surveillance en continue / 01-les réseaux et services réseaux sont surveillés)	**CIS-6** maintenance monitoring

	A.5.17 information d'authentification	**PR-AA-05 Gestion** des identités, authentification et contrôle d'accès / 05-integre le principe du moindre privilège	**CIS-04-14**
Justification	Les contrôles sélectionnés permettront de réduire les chances que l'attaquant trouve le mot de passe via l'haché car les mots de passes seront robustes. Il y aura également une activité de surveillance qui détectera tout mouvement suspect et la segmentation réseau limitera le périmètre (mouvement latéral impossible entre les segmentations).		
Statut :	Mise en œuvre		
Élément	**Détail**		
Risque	Phishing (intrusion dans les systèmes) et ingénierie sociale		
Choix de traitement	Réduction du risque		
Contrôles sélectionnés	Iso27001 :2022	Nist-CSF 2.0	Cis Controls v7
	A.6.3 sensibilisation et formation	**PR-AT-01 et 02** Sensibilisation et formation	**CIS-17** security skills and training
	A.8.7 protection contre logiciels malveillants	**DE.CM-09** Surveillance en continue/09-Le matériel et les logiciels sont surveillés	**CIS-7** email and browsing protect.
Justification	En s'assurant d'une formation et sensibilisation adéquate parallèlement à de bon système de détection/prévention des courriels et autres logiciels malveillant, nous nous assurons de réduire grandement les chances d'attaques et le succès des attaques.		
Statut :	Mise en œuvre.		

Annexe VI – Organigramme de la sécurité



Annexe VII – Diagrammes techniques



Annexe VIII – Scénario d'incidents

**Inspiré de l'attaque Talk-Talk, compagnie de télécommunication.*

Scénario 1- Exfiltration de données	**Scénario 2 – Phishing**	**Scénario 3- Injection SQL**
Menace : Attaquant utilise une commande pour extraire les données **Vulnérabilités :** pas de DLP, pas d'alertes **Impact** : Fuites des données, impact légal et réputationnel **Risque Brut** : Très Élevé **Risque Résiduel** : Moyen à élever (l'impact sera diminué avec une détection rapide)	**Menace :** Attaquant obtient les identifiants et mots de passe via l'hameçonnage **Vulnérabilités :** manque de formation / sensibilisation **Impact :** Compromission des données, confidentialité, intégrité **Risque Brut :** Très Élevé **Risque Résiduel :** Moyen à élever (la probabilité diminue)	**Menace :** Attaquant fait une extraction massive et accès non autorisé **Vulnérabilités** : système non patché – faille utilisée **Impact** : Fuite majeure, impact légal et réputationnel **Risque Brut :** Élevé **Risque Résiduel** : Faible à Moyen (si les systèmes sont à jour il sera plus difficile de trouver des failles)
Scénario 4 – Absence de chiffrement	**Scénario 5 – pas de segmentation réseau**	**Scénario 6 – mauvaise gestion des accès**
Menace : fuite de données alors que les données ne sont pas chiffrées **Vulnérabilités** : manque de chiffrement **Impact** : Confidentialité, légale, violation **Risque Brut** : Très Élevé **Risque Résiduel :** Faible à Moyen (les données seront chiffrées malgré une fuite)	**Menace** : Attaquant fait un mouvement latéral **Vulnérabilités** : manque de segmentation réseau **Impact** : Escalade de privilège, accès aux données **Risque Brut :** Élevé **Risque Résiduel** : Moyen (la probabilité que l'attaquant se déplace sera moindre)	**Menace** : Attaquant utilise un compte partagé, il ne se fait pas piéger **Vulnérabilités :** mauvaise gestion des accès / compromission d'un compte à privilèges **Impact :** Accès aux données sensibles, risque de corruption des données et fuite, impact légal **Risque Brut :** Très élevé **Risque Résiduel :** Moyen (la probabilité sera diminué, la non-répudiation entre aussi en jeu)
Scénario 7- Absence de surveillance	***Scénario 8 – Système non patché***	***Scénario 9 – Communication tardive***
***Menace** : Attaquant réussi des intrusions sans se faire détecter à plusieurs reprises* ***Vulnérabilités :** manque de surveillance des logs* ***Impact** : Énorme car l'attaquant exploitent à plusieurs reprises les failles, obtient plus de données*	***Menace :** Attaquant utilise une faille qui n'a pas été corrigé par les mises à jour* ***Vulnérabilités :** Système non patché* *Impact : Intrusion, accès aux données sensibles* ***Risque Brut** : Très élevé* ***Risque Résiduel** : Moyen*	***Menace** : L'entreprise tarde à annoncer la fuite à ses clients* ***Vulnérabilités :** Manque de communication externe* *Impact : réputationnel sévère, légal, risque de poursuite, les clients n'ont pas protégés leurs comptes assez rapidement*

clients, fuites, légal, réputationnel ***Risque Brut** : Très élevé* ***Risque Résiduel :** Moyen (L'attaquant sera détecté plus rapidement, ce qui réduira l'impact)*		***Risque Brut :** Très élevé* ***Risque Résiduel :** Moyen à Élevé (l'impact demeure mais moins réputationnel et risque légaux diminué)*
Scénario 10 – Mouvement latéral ***Menace :** Attaquant se déplace à travers le réseau* ***Vulnérabilités :** Mauvaise segmentation réseau* ***Impact :** élévation de privilège qui mène à un accès non autorisé* ***Risque Brut :** Très Élevé* ***Risque Résiduel** : Faible*	***Scénario 11 – Mauvaise réponse aux incidents*** ***Menace :** L'organisation n'a pas de plan de gestion des incidents, tout le monde panique et ne sait plus quoi faire* ***Vulnérabilités :** aucun plan de gestion de crise* ***Impact :** délai de contraignement augmenté, reprises tardives, impact financiers (employés qui travaillent plus lourdement) réputationnel* ***Risque Brut :** Très élevé* ***Risque Résiduel :** Moyen à faible* *(la réponse à l'incident sera plus rapide, l'impact sera diminué, les clients garderont confiance)*	***Scénario 12 – Mauvaise protection des comptes*** ***Menace** : Attaquant accèdent aux comptes car aucun MFA et mot de passe faibles* ***Vulnérabilités :** comptes mal protégés* ***Impact :** accès aux données sensibles, possible mouvement latéral* *Risque Brut : Très Élevé* *Risque Résiduel : Faible (l'attaquant a beaucoup moins de probabilité d'accéder au compte)*

Annexe IX – Classification des incidents

Niveau	Classification	RTO	RPO	Exemple
1	Mineur	48h-72h	24h	Verre d'eau tombé sur clavier
2	Moyen	16h-24h	4-8h	Compromission limitée
3	Majeur	4h-16h	30-60 minutes	Interruption des services, accès non autorisé
4	Critique	1h-4h	0-30 minutes	Fuite de donnée, ransomware, impact légale

Annexe X - Catégorisation et niveau de criticité

Niveau	Description	Exemple
Critique (Niveau 1)	Doit être restaurer immédiatement	AD, VPN, Serveur
Important (Niveau 2)	Reprise dans les 24h	CRM, Base de données
Non Critique	Reprise entre 48h et 72h	Services non essentiels

Annexe XI - Légende de niveau de criticité

Faible : Impact négligeable, perturbation mineure. Pas d'effet légal financier ou réputationnel.

Moyen : Impact notable, mais gérable. Gêne les opérations, coût modérés et atteinte à la réputation limitée.

Élevé : Impact significatif sur les opérations, réputations ou conformités. Perte financières importantes, atteinte à la réputation grave et risque légal.

Critique : Impact majeure ou catastrophique. Menace la survie de l'organisation et ou la sécurité des personnes.

Annexe XII – Cadre légal et normatif

Références légales :

- *Charte des droits et libertés de la personne du Québec* (R.LRQ., c. C-12);
- *Code civil du Québec* (L.Q., 1991, c. 64), (concernant notamment la protection de la réputation et de la vie privée ainsi que la communication des renseignements confidentiels);
- *Code criminel* (L.R.C., 1985, c. C-46), (concernant notamment l'interception frauduleuse d'informations, la falsification des documents et les méfaits);
- *Loi sur la protection des renseignements personnels et les documents électroniques S.C. 2000, c. 5 L.C. 2000, ch. 5*
- *Loi sur les télécommunications (LC 1993, ch.38)*
- *Loi sur la protection des renseignements personnels dans le secteur privé Chapitre P-39.1*;
- *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (Projet de loi no 64 (2021, chapitre 25);
- *Loi concernant le cadre juridique des technologies de l'information* (RLRQ., c. C-1.1) (concernant notamment la valeur juridique d'un document technologique et le maintien de l'intégrité durant tout son cycle de vie);
- *PCI DSS v4.0.1 Standard de sécurité des données*

Références Normatives :

- ISO/IEC 27001 :2022 *(Notre norme principale pour la gouvernance, notre leadership, nos objectifs et contrôles de sécurité (Annexe A), aide à la planification (clause 6), communication (clause 7).*
- ISO/IEC 27002 :2022 *(Notre norme d'implémentation pour les procédures, standard et directives)*
- ISO/IEC 27005 :2022 (*Notre norme pour la gestion du risque)*
- NIST CSF2.0/SP-800 *30/53/34/207 (Notre norme pour les opérations, réponse aux incidents, Zéro Trust, principe de défense en profondeur et le mapping ISO/NIST/CIS)*
- CIS CSC - *Critical Security Controls v.7.0 (Mapping ISO/NIST/CIS).*

Annexe XIII – détails sur les procédures

Annexe XII.1 Gestion des accès

Responsable de la procédure: DTI et CISO

Champ d'application: AD, VPN, Password Manager, Database, Application web et autre.

Voici les étapes pour la gestion des accès

1. La ressource humaine effectue une demande de création, modification ou ajout approuvé
2. Le TI crée le compte ou le rôle
3. Le CISO valide les permissions du rôle ou de l'utilisateur
4. L'utilisateur reçoit ses identifiants
5. Les rôles ou l'utilisateur est révoqué dans les heures suivant le départ

Référence: ISO27002:2022 8.2 et 8.3

Annexe XIII.2 Sauvegarde et restauration

Responsable de la procédure: DTI et CISO

Champ d'application: Serveur, Bases de données, AD et autres.

Voici les étapes pour la sauvegarde et restauration:

1. Exécution de la sauvegarde
2. Chiffrement de la sauvegarde
3. Application du 3-2-1 (3 Sauvegarde, 2 sur différent disque et 1 Hors site)
4. Vérification de l'intégrité
5. Test de restauration
6. Documentation

Références: ISO27002:2022 8.13 et NIST 800-34 3.4.1

Annexe XIII.3 Gestion des incidents

Responsable de la procédure: CISO

Champ d'application: SIEM, IDS/IPS, Antivirus, Serveur, réseau, applications, comptes d'utilisateur

Étapes:

1. Détection de l’incident
2. Classification de l’incident
3. Analyse de l’incident
4. Éradication de l’incident
5. Rétablissement à la suite de l’incident
6. Rapport post incident
7. Mise à jour du registre des incidents

Références: NIST CSF

Annexe XIII.4 Gestion des changements

Responsable: DTI et CISO

Champ d’application: Infrastructure réseau, serveur, configuration

Étapes:

1. Soumission de la demande de changement
2. Analyse des modifications
3. Analyse de risque
4. Approbation du changement
5. Implémentation des changements dans l'environnement de TEST
6. Correction des erreurs ou failles
7. Documentation du changement
8. Approbation et déplacement dans l’environnement de Production

Référence: ISO27002 8.32

Annexe XIII.5 Gestion des journaux et de la journalisation

Responsable: Soc, Infra

Champ d’application: SIEM, serveur, Firewall, VPN, AD, application, et autre

Étapes:

1. Collecte et agrégation des logs
2. Surveillance en continue des logs
3. Analyse des incidents potentiels
4. Escalade des informations
5. Audit de vérification
6. Conservation des logs et archivage

Référence: ISO 27002 8.15 et 8.16

Références

Références normatives

1. *Impact sur l'organisation* : Chapitre 10 Évaluation gestion et migration des risques selon la norme ISO 27001.pdf
2. Appréciation des conséquences potentielles (7.3.2) - ISO 27005: 2022.pdf
3. Identification d'un actif selon ISO 27005 – Gestion_des_actifs_Informationnels.pptx
4. ISO 27001: *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements.*
5. ISO 27002: *ISO/IEC 27002:2022 — Information security, cybersecurity and privacy protection — Information security controls.*
6. ISO 27005: *ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on information security risk management.*
7. ISO/IEC 27035-1 - *Technologies de l'information — Techniques de sécurité — Gestion des incidents de sécurité de l'information*
8. NIST.SP. 800 (34) *Contingency Planning*
9. NIST 800 (53-61) *Incident Response Recommendations and Considerations for Cybersecurity*
   Risk Management
10. NIST.SP.800-53r5 - *Security and Privacy Controls for Information Systems and Organizations*
11. NIST.SP.800-207 – *Zero Trust Architecture*
12. NIST.SP.800-*171 – Protecting Controlled Unclassified Information in Non-federal Systems and Organizations*
13. CIS CSC - *Critical Security Controls v.7.0*
14. Projet de session - https://cumberlandcollege.instructure.com/courses/419/files/14839?module_item_id=8468
15. H.LOM Chapitre 11 structure de la norme ISO 27001 et les phases de gestion des risques.pdf
16. https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=154#/

PSI de Bell :

17. https://www.bce.ca/responsabilite/documents-cles/2022-confidentialite-donnees-securite-information.pdf

PSI de Vidéotron (introuvables mais autres politiques Vidéotron et sujet relié et PSI dont nous nous sommes inspirés :

1. https://www.kbc.com/content/dam/kbccom/doc/sustainability-responsibility/OurApproach/CSR_OA_policy_policyprotectionlanceursd%27alerte.pdf
2. https://soutien.bell.ca/_web/guides/Common/Legal/Politique_de_Bell_sur_la_protection_de_la_vie_privee_FINALE.pdf
3. https://www.bell.ca/styles/common/fr/all_regions/pdf/SMBAcceptabeussefr.pdf

4. https://soutien.bell.ca/facturation-et-comptes/securite_et_confidentialite#right-panel
5. https://www.bce.ca/responsabilite/documents-cles/2022-confidentialite-donnees-securite-information.pdf
6. https://corpo.videotron.com/securite/vulnerabilite-web
7. https://corpo.videotron.com/confidentialite
8. https://www.videotron.com/affaires/ge/internet-reseaux/securite
9. https://www.ville.quebec.qc.ca/publications/docs_ville/politique_securite_information.pdf

Cas de fuite chez Videotron :

https://www.lapresse.ca/affaires/2023-08-03/la-securite-du-reseau-de-videotron-mise-en-peril-par-un-employe.php

Cas de ransomware chez Bell :

https://www.bleepingcomputer.com/news/security/hive-ransomware-claims-cyberattack-on-bell-canada-subsidiary/

Cas de fuite chez Talk ralk (phishing + intrusion)

https://open.spotify.com/episode/4fihCSOPKrIDXPB2azNgOc

Études sur les rôles et responsabilités :

https://rocketreach.co/bell-management_b5c61c29f42e0c49

https://corpo.cogeco.com/cgo/en/company-overview/management-team/

https://open.spotify.com/episode/0pdCe7iyZnVgDJ9fX3m35V

https://cyber.gouv.fr/publications/panorama-des-metiers-de-la-cybersecurite

https://www.quebec.ca/gouvernement/travailler-gouvernement/emplois-fonction-publique/domaines-emploi/technologies-information

https://www.fortinet.com/fr/resources/cyberglossary/devops-security

Mapping ISO/NIST/CIS:

10. https://www.censinet.com/perspectives/iso-27001-and-nist-csf-control-mapping-checklist
11. https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/mapping-and-compliance-with-the-cis-controls
12. https://csrc.nist.gov/projects/olir/informative-reference-catalog/details?referenceId=154#/
13. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.fre.pdf

Sources registre d'autorité

14. https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/emploi-solidarite-sociale/publications-adm/politiques-directives-procedures/PO_securite_information.pdf#:~:text=Registre d'autorité Recueil où sont notamment consignés,intervenants en matière de sécurité de l'information.