Centre de la sécurité des télécommunications | Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Guide de cybersécurité à l'intention des organismes électoraux

GESTIONNAIRES

Canada

AVANT-PROPOS

L'ITSM.10.021, *Guide de cybersécurité à l'intention des organismes électoraux,* est un document NON CLASSIFIÉ publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 26 août 2020.

HISTORIQUE DES RÉVISIONS

Version	Modifications	Date
1	Première version.	26 août 2020

VUE D'ENSEMBLE

Le présent guide de cybersécurité a pour objet de fournir des orientations aux organismes électoraux afin de les aider à prévoir et à atténuer les menaces propres aux processus démocratiques du Canada, et à y réagir. Il décrit les mesures de cybersécurité de base et les pratiques exemplaires qu'il convient de mettre en œuvre afin d'améliorer le profil de sécurité de votre organisme. Il établit également une série de normes auxquelles les organismes électoraux peuvent se référer pour continuer de renforcer les systèmes actuels et en mettre en place de nouveaux.

Les conseils formulés dans le présent document reposent sur des renseignements tirés de diverses sources et visent uniquement à établir une série de recommandations qui pourront être mises en œuvre dans le cadre des politiques et des pratiques actuelles de votre organisme.

Le présent document ne fournit pas d'orientations exhaustives sur les mesures que devrait prendre votre organisme pour contrer les cybermenaces. Il conviendra plutôt d'élaborer votre propre guide en tenant compte des considérations liées à la sécurité abordées dans le présent document ainsi que des besoins opérationnels et des exigences de sécurité de votre organisme.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

1 INTRODUCTION

Les organismes électoraux d'un bout à l'autre du Canada doivent prendre des dispositions afin de protéger les processus et systèmes démocratiques. Toute compromission éventuelle des données électorales viendrait nuire à la capacité des institutions démocratiques de s'acquitter de leur mandat et risque d'ébranler la confiance du public envers les résultats d'élections et les processus démocratiques. En 2016, la sécurité électorale a pris un tournant lorsque les tentatives visant à perturber les processus électoraux des États-Unis ont été rendues publiques. Des enjeux liés à l'intégrité des bulletins de vote, aux systèmes d'inscription des électeurs et aux mesures prises pour confirmer l'admissibilité des électeurs ont également été soulevés.

Au cours des dernières années, des cyberattaques ont été menées de manière à coïncider avec des élections partout dans le monde. Bien que les auteurs de menace aient employé toute une gamme de techniques dans le cadre de ces attaques, la majorité d'entre elles consistaient en attaques par déni de service distribué (DDoS pour *Distributed Denial of Service*) contre des sites Web de gouvernements et de médias. Lors d'une attaque par déni de service distribué, un auteur de menace tente d'interrompre l'accès à un site Web ou à un système en le submergeant de trafic. Les attaques constatées semblent avoir eu comme objectif de voler des données, de modifier les résultats d'élections et de perturber la publication de ces résultats.

Certaines des activités de menace signalées sont parfois associées à des activités de cybermenace et visent à influencer les électeurs ou à miner la confiance du public envers les résultats d'élections et les processus électoraux. Parmi ces tentatives, on compte les cyberactivités malveillantes constatées par le gouvernement des États-Unis au cours des élections présidentielles de 2016, ainsi que les présumés reportages frauduleux signalés récemment qui visent à influencer l'opinion publique.

Il convient de souligner que le présent document ne vise pas à fournir des conseils exhaustifs sur les mesures à prendre afin de protéger votre organisme contre les cybermenaces. Il constitue l'un des nombreux éléments d'un programme de cybersécurité et repose sur les orientations formulées dans l'ITSM.10.021, *Conseils en matière de cybersécurité à l'intention des organismes électoraux* [1].

1.1 GESTION DES RISQUES LIÉS À LA SÉCURITÉ DES TI

L'ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [2], décrit les rôles, les responsabilités et les activités que les organisations devraient mettre en œuvre afin de gérer les risques liés à la sécurité des TI. L'ITSG-33 [2] porte sur les principes clés ci-dessous :

- **Déterminer la sensibilité des actifs** : Identifiez les actifs de votre organisation et classez et catégorisez-les selon leur niveau de sensibilité en tenant compte des exigences législatives et réglementaires applicables[1], puis créez un répertoire indiquant où se trouvent vos actifs.

[1] Le Secrétariat du Conseil du Trésor du Canada (SCT) exige que les organismes du GC traitent l'information nominative (PII pour *Personally Identifiable Information*) selon le niveau de sensibilité moyen. Le SCT recommande également d'éviter de stocker les renseignements très sensibles (p. ex. les votes individuels) dans le nuage.

- **Cerner les menaces les plus importantes** : Déterminez qui ou quoi pose la menace la plus importante pour vos données. Votre organisme se préoccupe-t-il le plus d'auteurs de menace parrainés par un État, du crime organisé, de pirates individuels ou de la divulgation accidentelle? Plus l'auteur de menace est sophistiqué, plus vos mesures permettant de sécuriser vos données doivent être sophistiquées pour contrer ses attaques.
- **Comprendre les vulnérabilités qui touchent vos solutions informatiques** : Des organisations comme MITRE dressent des listes de vulnérabilités et expositions courantes (CVE pour *Common Vulnerabilities and Exposures*) qui touchent les technologies de l'information. Passez en revue la liste de MITRE ou d'autres listes semblables accessibles publiquement, et vérifiez si ces vulnérabilités connues touchent les solutions informatiques de votre organisme.
- **Déterminer les contrôles de sécurité appropriés** : Consultez le catalogue des contrôles de sécurité (à l'annexe 3A de l'ITSG-33 [2]) pour déterminer les contrôles de sécurité que vous devrez mettre en œuvre en fonction du niveau de sensibilité de vos actifs et des menaces et des vulnérabilités susceptibles de toucher votre organisme.

1.2 MESURES DE SÉCURITÉ PRÉVENTIVES

On a tendance à penser que la sécurité des TI constitue une solution à appliquer après la compromission d'un réseau, d'un système ou de l'information. Or, il ne s'agit pas uniquement d'une mesure d'intervention en réponse à une attaque, mais bien d'un processus continu consistant à prévenir et à détecter les menaces, puis à y répondre. Pour faire face aux menaces et aux vulnérabilités, nous vous recommandons de prendre des mesures de sécurité préventives en mettant en œuvre divers types de contrôles de sécurité en fonction de vos besoins et de vos exigences. À titre d'exemple, vous pouvez choisir des contrôles de sécurité parmi chacune des catégories ci-dessous pour vous aider à élaborer les mesures nécessaires pour protéger votre information :

- **contrôles de sécurité administratifs** : procédures mises en œuvre pour définir les rôles, les responsabilités, les politiques et les fonctions administratives nécessaires pour gérer un environnement (p. ex. les procédures d'embauche, la séparation des tâches);
- **contrôles de sécurité techniques** : solutions matérielles et logicielles mises en œuvre pour contrôler l'accès à l'information et aux réseaux (p. ex. systèmes de détection d'intrusion, pare-feux, logiciels antivirus);
- **contrôles de sécurité physiques** : contrôles visant à protéger les personnes et l'environnement physique (p. ex. serrures, garde-corps).

Vous trouverez un catalogue des contrôles de sécurité à l'annexe 3A de l'ITSG-33 [2]. Il conviendra de le consulter pour déterminer les contrôles que vous devrez appliquer en fonction des besoins et des exigences de votre organisme. Nous vous recommandons également de passer en revue l'ITSM.10.189 *: Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* [3], car ce document présente dix pratiques exemplaires à adopter pour sécuriser les réseaux et les systèmes.

2 SÉCURITÉ DES SYSTÈMES DE VOTE

Il est essentiel d'assurer la sécurité des modes de scrutin afin de protéger les processus démocratiques. Le tableau 1 ci-dessous décrit les mesures de sécurité recommandées par le Centre pour la cybersécurité qu'il convient de mettre en œuvre dans le cadre de votre programme de protection des systèmes de vote.

Les conseils formulés dans le présent document reposent sur des renseignements tirés de diverses sources et visent uniquement à établir une série de recommandations qui pourront être mises en œuvre dans le cadre des politiques et des pratiques actuelles de votre organisme.

Tableau 1 : Mesures de sécurité visant à protéger les systèmes de vote

Mesure de sécurité	Description
Séparation des réseaux (isolement)	L'isolement est une mesure de sécurité réseau consistant à isoler physiquement un réseau sécurisé des réseaux non sécurisés (comme Internet). À moins que ce soit absolument nécessaire, vous ne devriez pas connecter un système de vote à tout autre réseau, y compris les réseaux locaux et Internet. Si vous devez connecter des systèmes de vote à l'un de ces réseaux, il conviendra d'utiliser des dispositifs d'isolement comme des pare-feux et des solutions interdomaines.
Création des bulletins de vote	L'équipe chargée de créer les bulletins de vote devrait travailler dans une salle comportant des systèmes de surveillance et à laquelle l'accès est retreint à l'aide de laissez-passer à facteurs d'authentification multiples. Aucune connexion réseau ne doit se trouver dans cette salle.
Impression des bulletins de vote	Il convient d'imprimer les bulletins de vote en interne afin d'atténuer les risques qu'entraînerait la production des bulletins de vote par un fournisseur. Le bulletin de vote devrait être coloré et comporter un filigrane. S'il est impossible d'imprimer les bulletins de vote en interne, vous devez choisir un fournisseur digne de confiance.
Chaîne de possession	Il convient d'appliquer des contrôles stricts pour la chaîne de possession des bulletins de vote et des composantes liées au vote. La chaîne de possession assure le suivi des bulletins de vote et des composantes liées au vote tout au long de leur cycle de vie, c'est-à-dire la collecte, la conservation sécurisée et l'analyse. La chaîne de possession permet également d'établir avec certitude qui a traité cette information, la date et l'heure auxquelles celle-ci a été recueillie ou transférée, et les fins auxquelles l'information a été transférée[2].
Assurance des résultats des élections	Il convient de mettre en œuvre des mécanismes d'audit du dépouillement des votes pour en assurer l'exactitude, notamment au moyen de l'intégrité par deux personnes.
Tenue à jour de la liste d'électeurs	Il convient de fournir aux électeurs des instructions claires sur la manière de modifier leur adresse postale et leurs coordonnées. La mise à jour de la liste d'électeurs vous évitera d'envoyer l'information sur les électeurs à la mauvaise adresse.

[2] Définition tirée du glossaire du *Computer Security Resource Centre* [4] de la National Institute of Standards and Technology (NIST) [4]. Traduction libre.

Registre électronique du scrutin	Il convient d'utiliser un registre électronique du scrutin pour examiner et tenir à jour les renseignements sur les électeurs en prévision des élections. Le registre électronique du scrutin ne permet pas de compter les votes. Cette technologie peut permettre de remplacer ou de compléter les registres sur papier. Les représentants des organismes électoraux pourront consulter l'ensemble des données électorales ou celles d'un seul bureau de vote, selon leur niveau d'accès. Il convient également de chiffrer les communications transmises entre tous les dispositifs. Ces derniers doivent continuer d'être fonctionnels même si la connexion est interrompue. Les utilisateurs doivent arrêter tous les dispositifs lorsqu'ils ne les utilisent pas et les conserver en lieu sûr. Dans le cas des appareils mobiles, il convient d'envisager la mise en œuvre de mesures de gestion permettant d'assurer la sécurité des appareils et d'appliquer les stratégies nécessaires (p. ex. effacement à distance, listes d'applications autorisées et non autorisées, mise en œuvre du chiffrement des données, mises à jour logicielles).
Stockage de données en masse	Il convient de consulter l'ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* [5], afin de prendre connaissance des pratiques cryptographiques exemplaires à adopter pour stocker l'information recueillie auprès des électeurs (p. ex. les données inactives).
Services gérés et services infonuagiques	Si vous choisissez d'avoir recours à des services gérés ou infonuagiques, vous devrez vous assurer que les services du fournisseur ont été évalués et qu'ils sont en mesure de sécuriser les données. Vous devrez également définir clairement les niveaux de service attendus en ce qui concerne les rôles et les responsabilités liés à la sécurité des données. Visitez le site **cyber.gc.ca** pour trouver des publications sur les services gérés et les services infonuagiques. Pour de plus amples renseignements sur la sécurité liée aux services gérés et infonuagiques, prière de communiquer avec le centre d'appel.
Vote par anticipation à distance	Il convient de définir clairement les exigences liées au vote par anticipation à distance. Par exemple, dans le cas des systèmes de vote par anticipation à distance, vous devez veiller à ce que les données restent toujours chiffrées et mettre en œuvre des mesures cryptographiques approuvées par le GC pour les données en transit. Voir l'ITSP.40.062, *Conseils sur la configuration sécurisée des protocoles réseau* [6], pour en savoir plus.

3 SÉCURITÉ RÉSEAU

La sécurité réseau comporte les mesures mises en œuvre afin de protéger l'utilisabilité et l'intégrité de votre réseau et de vos données. La prise de mesures de cybersécurité de base peut contrer la plupart des attaques. Le fait de jumeler ces mesures à des analyses et à des audits périodiques des processus électoraux permet de réduire la capacité d'un auteur de cybermenace de causer des dommages d'envergure.

Pour éviter d'introduire d'autres risques opérationnels, nous vous recommandons de planifier attentivement et de mettre à l'essai tout changement à votre infrastructure ou aux solutions de votre fournisseur de services. Nous vous recommandons de mettre en œuvre les mesures de sécurité décrites dans le tableau 2 dans le cadre de votre programme de sécurité réseau.

Tableau 2 : Mesures de sécurité réseau

Mesure de sécurité	Description
Pare-feux	Installer des pare-feux pour surveiller les flux de trafic entrant et sortant du réseau.
Systèmes de détection et de prévention d'intrusion	Utiliser un système de détection et de prévention d'intrusion (IDPS pour *Intrusion Detection and Prevention System*). Ce système permettra de détecter les tentatives d'accès non autorisé et les activités malveillantes et vous enverra des alertes le cas échéant.
Contrôles de sécurité pour les justificatifs d'ouverture de session	Mettre en œuvre une stratégie de mot de passe, exiger l'utilisation de phrases de passe ou de mots de passe complexes, avoir recours à l'authentification multifactorielle et appliquer le principe du droit d'accès minimal afin de contrôler l'accès à vos systèmes. • Pour de plus amples renseignements sur les mots de passe et les phrases de passe, voir l'ITSAP.30.032, *Pratiques exemplaires de création de phrases de passe et de mots de passe* [7]. • L'authentification multifactorielle consiste à exiger au moins deux modes d'authentification (p. ex. un mot de passe et une caractéristique biométrique ou un mot de passe et un jeton). • Le principe du droit d'accès minimal consiste à accorder aux utilisateurs seulement les droits d'accès dont ils ont besoin pour exercer leurs tâches ou leurs fonctions.
Gestion des comptes d'utilisateur	Désactiver les comptes d'utilisateur dès qu'ils ne sont plus nécessaires.
Gestion des mises à jour de sécurité et des correctifs	Appliquer les correctifs et les mises à jour de sécurité en suivant votre processus de gestion des correctifs. Il convient de mettre à l'essai les correctifs et les mises à jour avant de les appliquer.
Renforcement des systèmes	Désactiver les services, les ports et les protocoles qui ne sont pas nécessaires.
Activation des fonctions de sécurité disponibles	Activer les options de sécurité renforcée offertes par les fournisseurs de vos logiciels et de vos systèmes (les options varieront selon l'architecture du système et le fournisseur).

sur les systèmes de votre organisation	
Systèmes hérités	Éviter d'utiliser des systèmes d'exploitation et des logiciels désuets et ceux qui ne sont plus pris en charge. Remplacer les systèmes hérités par des systèmes plus récents dans la mesure du possible.
Surveillance et évaluation continue de la sécurité	Mettre en œuvre un système de gestion des informations et des événements de sécurité (GIES) pour assurer la sécurité continue de vos réseaux et systèmes. Un système de GIES exécute des fonctions comme la détection d'intrusion, l'évaluation des vulnérabilités, la découverte et l'inventaire des actifs, l'analyse comportementale et la gestion des journaux.

4 SÉCURITÉ DU PERSONNEL

Toutes les personnes appelées à intervenir dans les processus électoraux (qu'il s'agisse de fonctionnaires du gouvernement ou de l'administration en question ou des titulaires de postes temporaires chargés de travailler aux bureaux de vote, de gérer le vote postal ou de compter les votes) ont la responsabilité de protéger la sécurité de vos réseaux, de vos systèmes et de votre information.

Tous les membres du personnel ont un rôle à jouer pour maintenir la confiance du public dans le processus électoral. Nous vous recommandons d'intégrer à votre programme de sécurité du personnel les mesures de sécurité décrites dans le tableau 3.

Les conseils formulés dans le présent document reposent sur des renseignements tirés de diverses sources et visent uniquement à établir une série de recommandations qui pourront être mises en œuvre dans le cadre des politiques et des pratiques actuelles de votre organisme.

Tableau 3 : Mesures de sécurité du personnel

Mesure de sécurité	Description
Procédures d'embauche axées sur la sécurité	Vérifier les antécédents des personnes que vous pensez embaucher. Pour de plus amples renseignements, prière de consulter la *Norme sur le filtrage de sécurité* du SCT [8].
Définition et gestion des rôles et responsabilités	Mettre en œuvre des politiques qui définissent clairement les rôles et les responsabilités.
Contrôles d'accès en fonction du niveau de confiance	Appliquer les principes du droit d'accès minimal et de la séparation des tâches pour veiller à ce que les employés puissent accéder uniquement aux systèmes et à l'information dont ils ont besoin pour remplir leurs fonctions.
Responsabilités liées à la sécurité physique	Tenir le personnel responsable de l'application des mesures de sécurité physiques. Établir dans vos politiques les comportements attendus et les répercussions liées à tout manquement.
Formation obligatoire sur la sécurité	Fournir de la formation obligatoire sur la cybersécurité et la sécurité électorale à tout le personnel, y compris les bénévoles. Votre formation devrait porter sur l'hameçonnage, le piratage psychologique, les attaques par rançongiciel, les maliciels, les lignes directrices sur les mots de passe, les procédures de sécurité physique, la sensibilisation à la protection de la vie privée et l'utilisation en toute sécurité des appareils mobiles et des réseaux sociaux.

5 INTERVENTION EN CAS D'INCIDENT

Même si vous avez pris des mesures de gestion des risques, des incidents pourraient se produire et compromettre la sécurité des processus électoraux et les données sensibles. Que ces incidents soient d'origine malveillante ou accidentelle, votre capacité d'y réagir efficacement aura une incidence sur l'étendue des dommages.

Votre organisme doit établir une stratégie d'intervention en cas d'incident qui repose sur le cycle de vie ci-dessous :

- **Planification** : Établir un processus et une stratégie d'intervention en cas d'incident qui tiennent compte de toute une gamme de considérations, notamment :
  - des mécanismes et des outils permettant de détecter, de confiner et d'éradiquer l'incident, puis de reprendre les activités et d'assurer le suivi nécessaire;
  - les rôles et responsabilités des employés, de la direction et de l'équipe d'intervention en cas d'incident;
  - l'établissement de rapports et les plans de communication;
  - les processus de reprise après sinistre et de continuité des activités.
- **Détection** : Déterminer les incidents possibles et ceux qui sont les plus susceptibles de toucher votre organisme et la manière dont celui-ci peut détecter ces situations dès qu'elles se produisent.
- **Confinement** : Déterminer les mesures qui seront prises afin de limiter les pertes (p. ex. dans le cas de vol d'information et d'interruption de services).
- **Éradication** : Déterminer les mesures qui seront prises afin d'éliminer la menace de votre infrastructure.
- **Reprise** : Déterminer les mesures qui seront prises afin de restaurer les services informatiques rapidement et en toute sécurité. Assurez-vous d'effectuer la sauvegarde de vos systèmes et de votre information pour que vous puissiez rétablir les systèmes touchés à leur dernier état valide. Faites l'essai de votre plan de reprise.
- **Suivi** : Établir un plan de communication, évaluer les mesures prises en réponse à des incidents antérieurs et consigner les « leçons tirées » ou les mesures de suivi.

Tout au long du cycle de vie de la gestion de l'incident, il convient de tenir compte des points suivants :

- **Communiquer** : Aviser toutes les parties concernées en interne et en externe, maintenir la connaissance de la situation et faire circuler les coordonnées en cas d'urgence dans le cadre des mesures d'intervention immédiates en cas d'incident.
- **Analyser** : Examiner les données disponibles à l'appui de la prise de décisions sur la façon de gérer l'incident.
- **Consigner** : Documenter tous les éléments de preuve (en notant la date et l'heure) ainsi que l'information et les mesures prises tout au long de la mise en œuvre du plan d'intervention en cas d'incident (c'est-à-dire dès la détection jusqu'à l'étape du suivi).

6 PARTENARIATS ET ÉCHANGE DE RENSEIGNEMENT

6.1 ÉCHANGE D'INFORMATION

Nous collaborons avec des organismes électoraux à l'échelle fédérale, provinciale et territoriale. Nous ne pouvons dévoiler l'information qui découle des consultations individuelles avec ces parties sans l'autorisation expresse de nos clients, mais ces consultations éclairent les avis et les conseils que nous formulons. Les connaissances acquises dans le cadre de ces activités sont prises en compte dans nos documents d'orientation.

Nous vous recommandons de mener des consultations auprès d'organismes électoraux de votre ordre de gouvernement (p. ex. consultations provinciales-territoriales). Comme ces organismes sont souvent confrontés aux mêmes enjeux de cybersécurité que vous, vous pourrez tenir compte des leçons qu'ils ont tirées pour renforcer la posture de sécurité de votre organisme.

6.2 GRC ET ORGANISMES LOCAUX D'APPLICATION DE LA LOI

Si vous croyez que des activités criminelles ou de l'ingérence touchent vos processus électoraux, veuillez communiquer avec la Gendarmerie royale du Canada (GRC) et votre organisme local d'application de la loi. Ces organismes peuvent également déployer des agents le jour des élections pour assurer la sécurité physique.

6.3 CENTRE ANTIFRAUDE DU CANADA

Si vous organisme est victime de fraude, par exemple si un auteur de menace se fait passer pour votre organisme, veuillez communiquer avec votre service de police local et en faire rapport en ligne par l'entremise du Système de signalement des fraudes du Centre antifraude du Canada.

7 COMMUNIQUEZ AVEC NOUS

Pour de plus amples renseignements sur la cybersécurité ou pour signaler un incident de cybersécurité, communiquez par téléphone ou par courriel avec le centre d'appel. Vous pouvez également consulter notre site Web pour trouver des publications sur toute une gamme de sujets liés à la cybersécurité.

Centre d'appel
www.cyber.gc.ca
contact@cyber.gc.ca
613-991-8700 ou 1-833-CYBER-88

8 CONTENU COMPLÉMENTAIRE

8.1 LISTE DES ABRÉVIATIONS

Terme	Définition
CST	Centre de la sécurité des télécommunications
GC	Gouvernement du Canada
GIES	Gestion des informations et des événements de sécurité
GRC	Gendarmerie royale du Canada
IDPS	Système de détection et de prévention d'intrusion (*Intrusion Detection and Prevention System*)
SCT	Secrétariat du Conseil du Trésor du Canada
TI	Technologies de l'information

8.2 GLOSSAIRE

Terme	Définition
Authentification	Processus permettant de vérifier l'identité d'un utilisateur ou d'une entité (comme une application) et de confirmer que sa demande d'accès est valide et légitime.
Chaîne de possession	Processus consistant à documenter le parcours des éléments de preuve tout au long de leur cycle de vie, c'est-à-dire les étapes de la collecte, de la conservation sécurisée et de l'analyse.
Confidentialité	Caractéristique de l'information sensible protégée contre tout accès non autorisé.
Cyberattaque	Recours à des techniques électroniques visant à perturber, à manipuler, à détruire ou à scruter clandestinement un système informatique, un réseau ou un dispositif.
Disponibilité	Caractéristique de l'information ou des systèmes qui sont accessibles aux personnes autorisées au moment où celles-ci en ont besoin. La disponibilité est un attribut des actifs informationnels, logiciels, et matériels (l'infrastructure et ses composantes). Il est également entendu que la disponibilité comprend la protection des actifs contre les accès non autorisés ou les compromissions.
Hameçonnage	Procédé par lequel une tierce partie tente de solliciter de l'information confidentielle appartenant à un individu, à un groupe ou à une organisation en les mystifiant ou en imitant une marque commerciale connue, souvent dans le but de réaliser des gains financiers. Les hameçonneurs incitent les utilisateurs à partager leurs renseignements personnels (numéros de cartes de crédit, données bancaires ou autres renseignements) afin de s'en servir pour commettre des actes frauduleux.
Intégrité	Aptitude à protéger l'information contre les modifications ou les suppressions non intentionnelles ou inopportunes. L'intégrité permet de savoir si l'information est conforme à ce qu'elle est censée être. L'intégrité s'applique également aux processus opérationnels, à la logique des applications logicielles, au matériel ainsi qu'au personnel.
Isolement	Mesure de sécurité réseau consistant à isoler physiquement un réseau sécurisé des réseaux non sécurisés (comme Internet).

Terme	Définition
Piratage psychologique	Attaque dans le cadre de laquelle un auteur de menace tente de manipuler sa cible pour l'amener à effectuer des opérations ou à divulguer de l'information sensible.
Rançongiciel	Type de maliciel qui empêche un utilisateur légitime d'accéder à des ressources (système ou données) jusqu'à ce qu'il ait payé une rançon.
Services gérés	Services fournis par un tiers consistant à gérer à distance l'infrastructure TI et les systèmes des utilisateurs au nom du client.
Services infonuagiques	Services fournis par une entreprise et mis à la disposition des utilisateurs à la demande par l'entremise d'Internet, par opposition aux services fournis à partir de l'environnement TI local du client.

8.3 RÉFÉRENCES

Numéro	Référence
1	Centre canadien pour la cybersécurité. *Conseils en matière de cybersécurité à l'intention des organismes électoraux* (ITSM.10.020), mai 2020.
2	Centre canadien pour la cybersécurité. *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (ITSG-33), novembre 2012.
3	Centre canadien pour la cybersécurité. *Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* (ITSM.10.189), octobre 2018.
4	National Institute for Standards and Technology. *Computer Security Resource Centre,* « Glossary ».
5	Centre canadien pour la cybersécurité. *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B* (ITSP.40.111), août 2016.
6	Centre canadien pour la cybersécurité. *Conseils sur la configuration sécurisée des protocoles réseau* (ITSP.40.062), août 2016.
7	Centre canadien pour la cybersécurité. *Pratiques exemplaires de création de phrases de passe et de mots de passe* (ITSAP.30.032), septembre 2019.
8	Secrétariat du Conseil du Trésor du Canada. *Norme sur le filtrage de sécurité*, octobre 2014.