# GUIDE CPA DES BONNES PRATIQUES D'UTILISATION DES TI

ORDRE DES COMPTABLES PROFESSIONNELS AGRÉÉS DU QUÉBEC



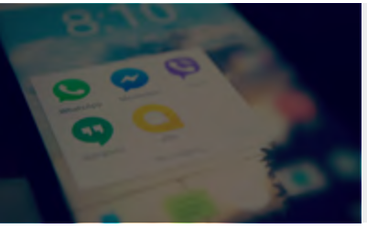






















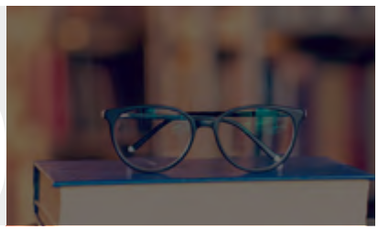




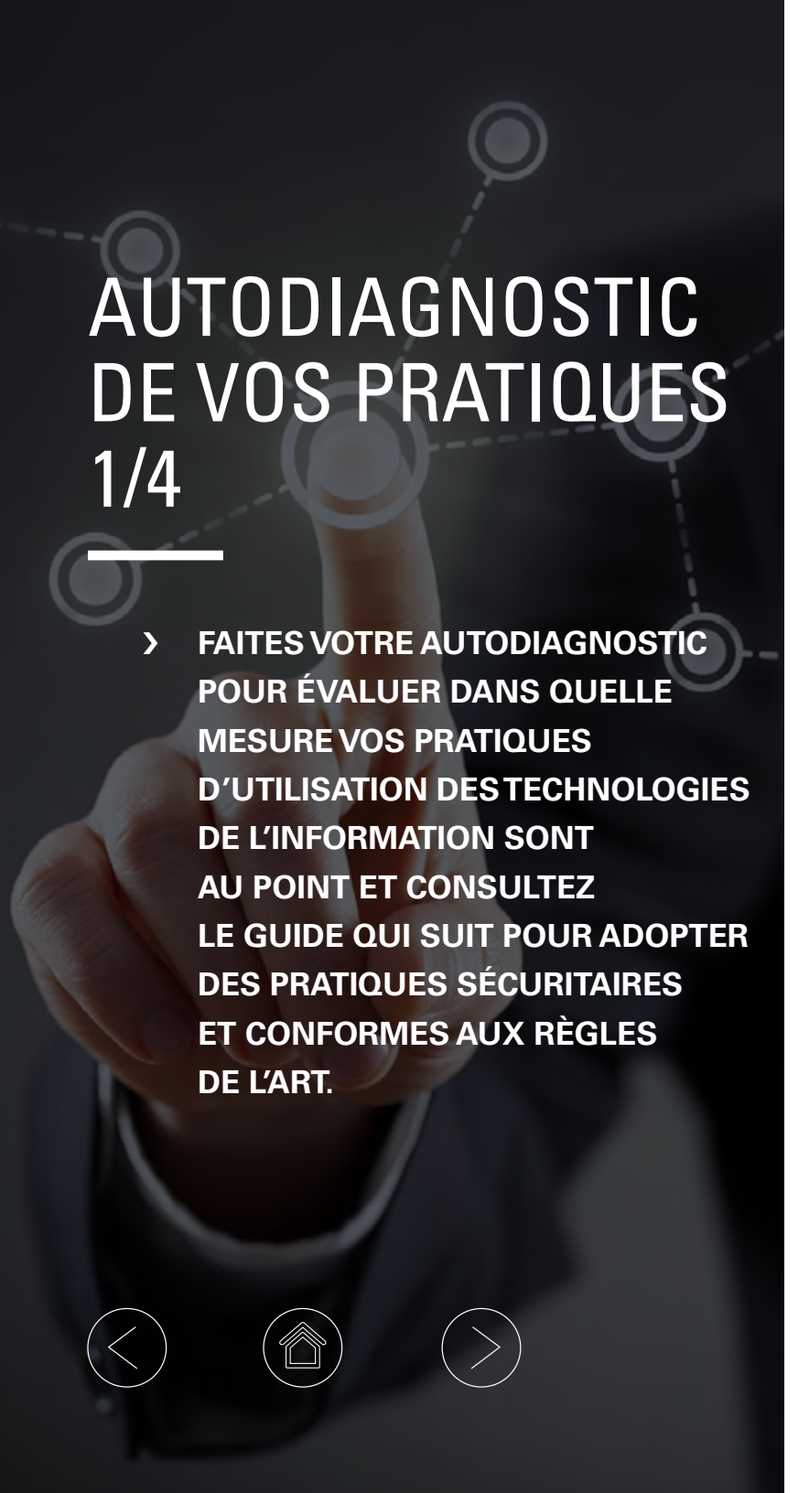








# TABLE DES MATIÈRES



# AUTODIAGNOSTIC DE VOS PRATIQUES 1/4

› **FAITES VOTRE AUTODIAGNOSTIC POUR ÉVALUER DANS QUELLE MESURE VOS PRATIQUES D'UTILISATION DES TECHNOLOGIES DE L'INFORMATION SONT AU POINT ET CONSULTEZ LE GUIDE QUI SUIT POUR ADOPTER DES PRATIQUES SÉCURITAIRES ET CONFORMES AUX RÈGLES DE L'ART.**

## Une question vous interpelle? Cliquez et suivez le guide.

L'accès à votre poste de travail est-il protégé par un nom d'usager et un mot de passe ?

Les mots de passe sont-ils suffisamment sécuritaires ?

Votre poste de travail est-il mis en veille automatiquement après un certain laps de temps ?

Le nom d'usager et le mot de passe donnant accès à votre poste de travail sont-ils partagés ou conservés dans un endroit accessible à un membre de votre cabinet ou à votre employeur en cas de décès ou d'incapacité subite ?

Les accès sont-ils protégés par une authentification multi-facteurs?

Votre poste de travail est-il protégé par un antivirus mis à jour de façon automatisée ?

Les disques durs des ordinateurs portables sont-ils chiffrés ?

Votre organisation a-t-elle un programme de formation et de sensibilisation des employés en lien avec les politiques, lignes directrices et procédures concernant la sécurité ?

Ces politiques, lignes directrices et procédures sont-elles diffusées auprès des employés ?

Lors du départ d'un employé, les accès qui lui étaient accordés (serveur, comptes, documents) sont-ils supprimés afin d'assurer la confidentialité des données ?

Avez-vous mis en place une méthode de gestion des copies de sauvegarde des données (renseignements relatifs à vos clients) enregistrées sur votre réseau ?

Savez-vous à quelle fréquence sont sauvegardées les données ?

Savez-vous à quel endroit les copies de sauvegarde sont conservées ?

Ces copies de sauvegarde sont-elles chiffrées ou protégées par un mot de passe adéquat ?

Poursuivez votre autodiagnostic →

# AUTODIAGNOSTIC DE VOS PRATIQUES 2/4

Savez-vous si ces données sauvegardées seront récupérables dans un format qui sera lisible lorsque viendra le temps de les consulter, à court terme ?

Les données sont-elles hébergées dans un environnement hébergé ou infonuagique, ou sur un réseau local ?

Si vous utilisez un réseau local, ce réseau est-il protégé par un pare-feu mis à jour régulièrement ?

La sécurité physique de ce serveur est-elle assurée ?

Si l'accès à un réseau est offert à des visiteurs, ce réseau est-il distinct de celui donnant accès aux données ?

Lorsque vous faites affaire avec un consultant externe ou interne qui peut avoir accès aux données relatives à vos clients contenues dans votre système informatique (réseau interne, poste de travail, ordinateur mobile, téléphone intelligent, environnement hébergé et infonuagique, ou autre), lui faites-vous signer un engagement de confidentialité ?

Si les données sont hébergées à l'externe, un contrat a-t-il été conclu avec le fournisseur d'infonuagique ?

Ce contrat prévoit-il:

- des mesures assurant la confidentialité des données hébergées ?
- des mesures assurant l'intégrité des données hébergées ?
- des mesures encadrant l'accessibilité des données hébergées, vous permettant d'y avoir accès en tout temps ?
- un processus de destruction des données et des mesures quant à leur conservation ?
- un processus lié à la récupération des données hébergées et qui en garantit la valeur et l'intégrité ?
- un calendrier de sauvegardes et leur conservation ?

Ce contrat comporte-t-il une clause :

- assurant que vous ou votre employeur demeurez propriétaire des données hébergées et que celles-ci seront détruites à la fin du contrat ?
- obligeant le fournisseur à vous aviser en cas de vol de données ou de brèche ?
- permettant d'effectuer des audits ou de recevoir les résultats des audits effectués ?
- de couverture d'assurance en cas de perte de données ?

Les clients sont-ils informés que des données les concernant sont sauvegardées sur un serveur externe ?

Les données sont-elles hébergées en territoire canadien et le fournisseur est-il de propriété canadienne ?

Poursuivez votre autodiagnostic →

# AUTODIAGNOSTIC DE VOS PRATIQUES 3/4

Si vous avez recours à une plateforme de services (portail ou échange de fichiers) qui est accessible à vos clients, avez-vous mis en place des mesures pour en assurer la sécurité ?

Si vous communiquez avec vos clients ou votre employeur par courriel, savez-vous si le serveur que vous utilisez garantit la confidentialité et utilise un système de chiffrement ?

Chiffrez-vous les messages et les documents transmis par courriel ?

Obtenez-vous l'autorisation de vos clients avant d'échanger des informations confidentielles par courriel avec eux ?

Si vous transmettez des informations confidentielles par texto, comment vous assurez-vous qu'elles demeurent confidentielles ?

Votre téléphone intelligent contient-il des données relatives à vos clients ou des données de votre employeur ?

Les données contenues sur des plateformes mobiles (ordinateur portable, tablette, clé USB, disque dur externe, etc.) sont-elles suffisamment protégées et même chiffrées ?

Vous arrive-t-il d'utiliser des réseaux publics non sécurisés avec une plateforme mobile contenant des données relatives à vos clients ou à votre employeur ?

Votre organisation permet-elle à ses employés d'utiliser des appareils personnels et si oui, ces appareils doivent-ils respecter des exigences de sécurité (antivirus à jour, chiffrement des données et mots de passe robustes et changés fréquemment) ?

Une politique sur l'utilisation de ces technologies et qui prévoit les mesures de sécurité requises a-t-elle été mise en place ?

Disposez-vous de moyens de sécurité suffisants pour les employés qui se connectent à distance (ex. : accès VPN) ?

Lorsqu'un accès à distance est utilisé, à domicile par exemple, comment s'assure-t-on que le réseau Internet du domicile est sécurisé et que des données professionnelles ne puissent s'y retrouver ?

Votre organisation permet-elle le téléchargement d'un fort volume de données provenant de ses systèmes ?

Poursuivez votre autodiagnostic →

# AUTODIAGNOSTIC DE VOS PRATIQUES 4/4

Votre appareil mobile recherche-t-il automatiquement de nouvelles connexions Wi-Fi ou Bluetooth, sans votre intervention ?

Votre mot de passe contient-il un mot présent dans le dictionnaire ?

Utilisez-vous les paramètres par défaut d'un outil de collaboration en ligne ?

Qui est responsable de communiquer avec les clients en cas de cyberattaque touchant leurs données ?

Avez-vous une politique d'utilisation des médias sociaux qui s'applique à tous les employés de l'organisation ?

Connaissez-vous vos obligations en vertu du nouveau cadre législatif de la protection des renseignements personnels et de la gestion des données au Québec ?

1

# INTRODUCTION

Ce guide jette les bases du cadre d'utilisation des technologies de l'information dans l'exercice de la profession de CPA. Dès lors qu'il utilise un programme installé sur un ordinateur, un téléphone intelligent, le courriel ou un service hébergé en infonuagique, tout CPA est en effet exposé à des risques technologiques contre lesquels il doit mettre en place des mesures de mitigation appropriées.

Ce guide pratique met donc en lumière certains enjeux de sécurité liés à l'utilisation des technologies de l'information au quotidien et présente les bonnes pratiques à adopter pour en assurer la gestion en tenant compte des obligations déontologiques et réglementaires du CPA.


DEVOIR DE COMPÉTENCE ET DE CONSEIL

RESPECT DU SECRET PROFESSIONNEL

PROTECTION DES RENSEIGNEMENTS PERSONNELS

RÈGLES EN MATIÈRE DE PUBLICITÉ

Retour à l'autodiagnostic

# 1 INTRODUCTION

Retour à l'autodiagnostic

## Devoir de compétence et de conseil

Comme tout professionnel, le CPA a un devoir général de compétence. Pour s'en acquitter, il doit avoir acquis de vastes connaissances, qui vont au-delà de la maîtrise des règles comptables, et qui incluent les obligations déontologiques associées à l'exercice de la profession. Qu'il offre ou non des services à des tiers, le CPA doit se tenir au courant des développements et maintenir sa compétence dans les domaines où il exerce sa profession. Le devoir de compétence est assorti du devoir de conseil qu'a le CPA envers son client (qui peut être son employeur).

## Respect du secret professionnel

Tout CPA est tenu au secret professionnel et ne peut divulguer les renseignements confidentiels qui lui ont été révélés en raison de sa profession à moins qu'il n'y soit autorisé par celui qui lui a fait des confidences (son client) ou par une disposition expresse de la loi. En plus d'être encadré par le *Code des professions* et le *Code de déontologie des CPA*, le droit au secret professionnel est reconnu par la *Charte des droits et libertés de la personne*, qui prévoit aussi l'obligation pour tout professionnel de le respecter.

L'utilisation des technologies de l'information peut avoir une incidence directe sur le secret professionnel. Il est donc essentiel que le CPA soit conscient de ses obligations et de la sensibilité des informations qu'il détient, tant aux fins de leur conservation que de leur transfert ou de leur destruction afin d'éviter une divulgation involontaire. Qu'elles soient sur support papier ou électronique, le CPA doit protéger la confidentialité de ces informations et s'assurer que seules les personnes autorisées y aient accès. Ce guide identifie plusieurs situations où les points d'accès peuvent être fragilisés et propose des mesures de mitigation.

L'exercice de la profession en solo et l'utilisation de dossiers papier limitent l'exposition aux risques en matière de confidentialité. À l'inverse, le nombre de collaborateurs, les modalités de ces collaborations, ainsi que l'utilisation de réseaux (cellulaires, internet, applications et serveurs distants) font éclater le périmètre de sécurité. Le nombre de points d'accès à contrôler augmente d'autant.

De la même façon qu'un CPA ne saurait tenir une rencontre dans un lieu public au vu et au su de tous, il doit transposer cette discrétion en ligne- ce qui implique la compréhension de notions de sécurité de l'information et de l'environnement qu'il entend utiliser.

Dans les faits, cela signifie que tout CPA doit être en mesure d'identifier les situations à risque et que, face à un risque découlant de l'utilisation des technologies de l'information (par exemple, les communications par courriel), il doit en informer son client.

# 1 INTRODUCTION

Retour à l'autodiagnostic

## Protection des renseignements personnels

En plus de devoir respecter le secret professionnel auquel son client a droit, le CPA doit veiller à protéger les renseignements personnels qui lui sont transmis dans le cadre de l'exercice de la profession, quel que soit le support sur lequel sont conservés ces renseignements et quelle que soit la forme sous laquelle ils sont accessibles (écrite, graphique, sonore, visuelle, informatisée ou autre).

Qu'est-ce qu'un renseignement personnel?

Au Québec[1], tout renseignement qui concerne une personne physique et permet de l'identifier, directement ou indirectement. Il peut donc s'agir, par exemple, du numéro d'assurance sociale, des habitudes et de l'historique d'achats, de l'adresse IP, des opinions politiques ou des caractéristiques individuelles d'une personne.

Les renseignements personnels doivent être protégés contre l'intrusion et, sauf en cas d'exceptions prévues par la loi, ils ne peuvent être communiqués à des tiers qu'avec le consentement du client.

En pratique, le CPA doit donc :

- Protéger l'information qui lui est confiée ou à laquelle il a accès contre un bris potentiel de confidentialité en s'assurant d'un environnement sécuritaire.
- Connaître, au moins minimalement, les fonctions des technologies utilisées selon que le message est public ou privé.
- Reconnaître les situations qui mettent en péril la sécurité de l'information.
- Adopter les bonnes mesures de mitigation pour limiter ces risques.
- Connaître les limites de ses connaissances et compétences et recourir au besoin à des spécialistes pour sécuriser ses serveurs.
- Obtenir le consentement de son client avant de transférer de l'information à des tiers ou d'utiliser une technologie particulière visant à échanger de l'information.
- S'enquérir des avancées technologiques et s'assurer que sa solution technologique est appropriée et à jour.

## Règles en matière de publicité

Le CPA est soumis à des règles en matière de publicité. Il ne peut s'attribuer ou permettre que lui soient attribuées des qualités ou habiletés particulières en ce qui concerne, par exemple, son niveau de compétence ou l'étendue de ses services qu'il ne serait pas en mesure de justifier. Il doit donc être prudent et mesurer ses propos quant à l'information qu'il affiche sur son site Web ou les médias sociaux pour ne pas induire le public en erreur sur ses compétences ou celles de son cabinet. Il ne peut non plus faire ou permettre que soit faite de la publicité fausse ou trompeuse, incomplète ou qui va à l'encontre de l'honneur ou de la dignité de la profession.

Ces obligations s'appliquent quel que soit le médium utilisé. Considérant que le site Web du CPA (ou son profil sur un média social) est un outil promotionnel (donc un outil qu'il contrôle), les commentaires affichés par des tiers pourraient le placer en contravention de son obligation.

Le CPA doit donc filtrer les commentaires de tiers et apporter les correctifs nécessaires avant leur publication dans un environnement qu'il contrôle ou, si ce n'est pas possible, procéder régulièrement au filtrage des commentaires après leur publication.

[1] Voyez en annexe en quoi la ***Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*** modifie l'encadrement applicable à la protection des informations person-nelles, ainsi qu'à la cueillette, la conservation, l'utilisation, la communication et la destruction des données.

2

# PRINCIPES DE LA SÉCURITÉ DE L'INFORMATION

PRINCIPES CARDINAUX

PROTECTION DES ACTIFS INFORMATIONNELS CRITIQUES

Retour à l'autodiagnostic

2

# PRINCIPES DE LA SÉCURITÉ DE L'INFORMATION

## › PRINCIPES CARDINAUX

La disponibilité, l'intégrité et la confidentialité sont les principes cardinaux de la sécurité de l'information.

La **disponibilité** implique que les ressources informationnelles sont accessibles en temps utile à tout utilisateur autorisé. Une rupture de l'accès internet, accidentelle ou due à une attaque en déni de service, ou encore une prise de contrôle au moyen d'un rançongiciel (maliciel qui vient chiffrer le contenu d'un disque dur pour ensuite vendre la clé de déchiffrement à la victime) sont des causes possibles de ralentissement ou de blocage des activités commerciales ou professionnelles.

L'**intégrité** confirme qu'un document ou un dossier n'a été ni altéré ni amputé depuis sa création. Il s'agit d'un critère fondamental en droit civil québécois lorsque l'on entend faire admettre un document en preuve devant une instance décisionnelle.

L'intégrité va de pair avec la **traçabilité**. Elle permet de reconstituer ou de retracer le cheminement de l'information. De simples utilitaires gratuits permettent de valider qu'un document n'a pas été altéré (volontairement ou non) lors d'une communication en comparant la valeur de hachage à l'envoi et à la réception.

La **confidentialité** doit être préservée, tant au stade de la conservation du document que de sa transmission. Cela implique la mise en place de mesures de protection et de gestion du risque. Pour assurer la confidentialité d'une pièce jointe à un courriel (dont le contenu circule en clair sur internet), il est possible de chiffrer le document et de communiquer le mot de passe par téléphone ou courriel séparé. Une mesure plus efficace encore consiste à placer le document sur une plateforme d'échange sécurisée et à envoyer une notification au destinataire afin qu'il aille l'y chercher.

Retour à l'autodiagnostic

2

# PRINCIPES DE LA SÉCURITÉ DE L'INFORMATION

## › PROTECTION DES ACTIFS INFORMATIONNELS CRITIQUES

L'identification des types d'actifs informationnels à protéger est une étape essentielle de la mise en place d'un cadre de sécurité. À cette fin, il faut définir le niveau de criticité des actifs informationnels en fonction des trois principes de sécurité : la disponibilité, l'intégrité (qui inclut la traçabilité) et la confidentialité. Les actifs informationnels critiques comprennent :

- les renseignements protégés par le secret professionnel et ceux couverts par la législation en matière de protection des renseignements personnels, et particulièrement ceux qui sont identifiés comme étant sensibles en vertu de la législation[2] ;
- les procédés et méthodes développés pour assurer la prestation des services.

Les actifs informationnels peuvent être soumis à divers types de menaces :

- humaines, tant de source interne qu'externe (piratage, vol de données);
- naturelles (inondations, tempêtes solaires, tremblements de terre);
- techniques (bogues);
- physiques (bris, désuétude) parce qu'ils peuvent être utilisés à des fins frauduleuses.

### BONNES PRATIQUES

- Promouvoir une saine culture de sécurité de l'information en instaurant une politique d'utilisation des TI et des médias sociaux pour tous les employés de l'organisation.
- Identifier les actifs informationnels critiques en fonction de leur sensibilité.
- Évaluer périodiquement les risques relatifs à la sécurité de l'information en faisant appel au besoin à des experts au fait de l'évolution des enjeux de sécurité.
- Déterminer les mécanismes de sécurité nécessaires pour réduire la vulnérabilité de l'organisation à un niveau qu'elle juge approprié.
- Documenter les actions entreprises, en mesurer l'efficacité et mettre en œuvre les correctifs appropriés.
- Mettre en place un processus de gestion des risques (ligne directrice, procédures et processus) associé au cycle de vie de l'information : création, utilisation, conservation, communication et destruction.
- Veiller à la mise en pratique du cadre établi (ex. : audits, attestation annuelle).
- Considérer la possibilité de souscrire une assurance contre les cyberrisques.
- Considérer la pertinence, selon la taille de l'organisation, d'implanter une ligne de signalement de possibles manquements accessible tant aux employés qu'aux clients et fournisseurs.

Retour à l'autodiagnostic

[2] Au Québec, l'entrée en vigueur des dispositions de la ***Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*** se poursuit progressivement jusqu'en 2024. Voyez en annexe comment cette loi modifie l'encadrement applicable à la protection des informations personnelles, ainsi qu'à la cueillette, la conservation, l'utilisation, la communication et la destruction des données.

3

# SÉCURITÉ DE L'ENVIRONNEMENT

| | | | | |
|---|---|---|---|---|
| PÉRIMÈTRE DE SÉCURITÉ | SÉCURISATION DES POINTS D'ENTRÉE<br>SENSIBILISATION DES EMPLOYÉS | SÉCURISATION DES POINTS D'ENTRÉE<br>PARE-FEU | SÉCURISATION DES POINTS D'ENTRÉE<br>LOGICIEL ANTIVIRUS | SÉCURISATION DES POINTS D'ENTRÉE<br>BLOCAGE DE CERTAINS TYPES DE FICHIERS, APPLICATIONS ET PLUGICIELS |
| SÉCURISATION DES POINTS D'ENTRÉE<br>PÉRIPHÉRIQUES MALVEILLANTS | SÉCURISATION DES POINTS D'ENTRÉE<br>ÉVALUATION DES VULNÉRABILITÉS | SÉCURISATION DES POINTS D'ENTRÉE<br>GESTION DES MISES À JOUR | SÉCURISATION DES POINTS D'ENTRÉE<br>SURVEILLANCE ET GESTION DES ALERTES | |

Retour à l'autodiagnostic

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › PÉRIMÈTRE DE SÉCURITÉ

La notion de périmètre de sécurité est importante puisqu'elle sert à délimiter la portée des moyens à mettre en place pour bien protéger l'information.

Ainsi, le périmètre de sécurité d'un ordinateur sans connexion est limité aux quatre coins de la pièce. Si l'ordinateur est connecté à un serveur dans une autre pièce, le périmètre s'étend à cette autre pièce et il faudra le sécuriser par une mesure quelconque – garde de sécurité ou simple serrure. Si la connexion est sans-fil, les signaux devront être chiffrés, c'est-à-dire rendus inintelligibles à quiconque n'y est pas autorisé.

Le périmètre s'élargit aussi à toute personne qui collabore avec un CPA dans l'exercice de sa profession et à toute personne qui partage son espace de travail. S'il s'agit de fournisseurs externes, la vérification des pratiques de confidentialité est nécessaire et l'entente de service doit prévoir la protection de l'information.

Si l'on ajoute un téléphone intelligent qui contient des documents de travail et qui utilise des applications de communication avec la clientèle, le périmètre s'étend en fonction du nombre d'applications qui, une fois activées, auront accès à certaines informations stockées dans l'appareil (contacts, fichiers, historiques, données de localisation, etc.). Par exemple, activer la localisation (par GPS ou autre) pourrait révéler le nom d'un client à une application installée sur l'appareil.

Finalement, les appareils connectés au même réseau qu'un appareil professionnel pourraient aussi faire partie du périmètre à sécuriser. On peut penser aux téléphones intelligents des enfants qui sont connectés au réseau sans-fil familial, ou au réfrigérateur qui utilise ce même réseau. Des paramètres de sécurité insuffisants peuvent transformer ces appareils en points d'entrée sur le réseau.

Retour à l'autodiagnostic

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › SÉCURISATION DES POINTS D'ENTRÉE

### SENSIBILISATION DES EMPLOYÉS

Retour à l'autodiagnostic

Aucune méthode ou technologie ne peut prémunir une organisation contre l'ensemble des comportements négligents possibles. Si l'action humaine constitue la meilleure ligne de défense, celle-ci est aussi le plus grand facteur de risque pour la sécurité. Le développement de réflexes adéquats chez les employés constitue le meilleur filet de protection pour éviter une atteinte aux actifs informationnels de l'organisation.

### BONNES PRATIQUES

> Porter une attention particulière aux éléments suivants lors de la réception de courriels et de textos :
  - Reconnaissez-vous le nom et adresse de l'expéditeur?
  - Recevez-vous cette communication dans une langue autre que celle qui est habituellement employée par cet expéditeur?
  - Le courriel contient-il des fautes d'orthographe? Un courriel provenant d'une source fiable comme une banque ou une agence gouvernementale ne devrait pas comporter d'erreurs flagrantes.
  - Y a-t-il concordance entre l'adresse de l'expéditeur et l'adresse de réponse?
> Placer votre souris au-dessus d'un hyperlien sans cliquer dessus afin de vérifier l'URL de destination de ce lien et ainsi vérifier si celle-ci pointe vers un site fiable.
> Se méfier de la présence d'un ton pressant et confidentiel dans un message, de même que de toute demande inhabituelle de transmission d'information sensible.
> S'assurer que l'adresse des sites visités commence par « https:// » et non par « http:// ».
> Définir ce qui constitue dans votre organisation une utilisation justifiée des médias sociaux dans un cadre professionnel, par exemple pour le recrutement de personnel ou le développement des affaires, par opposition à une utilisation à des fins personnelles.
> Encadrer l'utilisation des médias sociaux en intégrant cette notion dans le code d'éthique à l'intention de votre personnel, notamment en ce qui concerne les publications qui pourraient nuire à la réputation de l'organisation, les fuites de secrets commerciaux, l'information au sujet de projets passés, présents ou futurs et le partage de renseignements sur l'organisation et ses parties prenantes.

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › SÉCURISATION DES POINTS D'ENTRÉE

### PARE-FEU

Retour à l'autodiagnostic

Le pare-feu s'intercale entre le système informatique que l'on cherche à protéger et un autre système informatique dont on cherche à se protéger. Le pare-feu fonctionne en créant des zones de confiance, en ségrégant les requêtes en provenance du réseau local et les requêtes du réseau externe, puis en bloquant certains canaux de communication pour n'en autoriser que certains jugés fiables.

### BONNES PRATIQUES

> Se doter d'un pare-feu, le configurer correctement selon les besoins de l'organisation et le tenir à jour. Le recours à des professionnels de la réseautique peut être nécessaire, selon la complexité du réseau (présence ou non d'extranet, d'un réseau privé virtuel, de serveurs Web ou courriel, etc.) et la taille de l'organisation.

> S'assurer que le pare-feu demeure activé en tout temps. Mettre en place un processus d'approbation préalable pour autoriser la désactivation du pare-feu lorsque la situation le justifie et veiller à le réactiver ensuite.

> S'assurer que le pare-feu est maintenu à jour avec les dernières versions disponibles afin de réduire les vulnérabilités.

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › SÉCURISATION DES POINTS D'ENTRÉE

### LOGICIEL ANTIVIRUS

Retour à l'autodiagnostic

La complexité des virus et autres maliciels (code malveillant) rend impérative l'utilisation d'un logiciel antivirus et antimaliciels. Ce logiciel est un outil de prévention d'actes illicites tels que :

- exfiltrer de l'information ;
- bloquer l'accès à l'information puis extorquer la victime pour qu'elle puisse la récupérer ;
- piéger la victime selon des stratagèmes frauduleux à complexité variable, pouvant aller jusqu'à l'envoi d'un maliciel ciblant une personne occupant une fonction précise dans une organisation. Par exemple, amener la victime à ouvrir une pièce jointe de provenance inconnue (un faux récépissé de livraison par messagerie privée), à cliquer vers un site infecté (souvent à la suite d'une attaque de type hameçonnage et à l'occasion cible une personne précise) ou à brancher un support amovible inconnu (une clé USB comportant un logiciel malveillant).

### BONNES PRATIQUES

- Se doter d'un logiciel antivirus et antimaliciels, le configurer correctement, le maintenir activé en tout temps et le tenir à jour, de préférence automatiquement.
- Sensibiliser les employés aux différents types de menace informatique, le vecteur usuel des virus et maliciels étant l'action humaine.

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › SÉCURISATION DES POINTS D'ENTRÉE

### BLOCAGE DE CERTAINS TYPES DE FICHIERS, APPLICATIONS ET PLUGICIELS

Retour à l'autodiagnostic

Les virus et autres maliciels utilisent des vecteurs généralement connus et contre lesquels il est relativement aisé de se prémunir. Ainsi, les pièces jointes comprenant des fichiers exécutables (contenant un programme directement exécutable par le processeur et permettant de lancer une application ou une commande) ou des fichiers comprenant eux-mêmes du code exécutable (tel une macro) doivent être bloqués ou à défaut, faire l'objet d'un blocage réversible dans les applications (par exemple, un fichier dont certaines fonctionnalités, telles que les macros, ne peuvent être activées que par une action de l'utilisateur, qui confirmera que la pièce jointe provient d'une source fiable).

### BONNES PRATIQUES

- Dans la configuration des serveurs courriel, bloquer les fichiers exécutables ou compressés dans les pièces jointes (*.exe, *.bat, *.msi, .zip, .rar, etc.).
- Configurer les filtres anti-pourriel pour bloquer les tentatives d'hameçonnage et les pièces jointes malveillantes.
- Désactiver par défaut les macros et autres codes exécutables dans les fichiers qui peuvent en comporter : logiciel de traitement de texte, tableurs, bases de données, fichiers PDF, etc.
- Aviser le personnel de n'ouvrir les fichiers, puis de n'activer les macros, que s'ils font confiance à l'expéditeur.
- Bloquer certaines applications et plugiciels reconnus pour leur faiblesse en matière de sécurité de l'information, même s'ils sont fréquemment mis à jour (Flash, Java, barres de recherche, fonds d'écran, etc.).
- Se tenir à jour quant à ce type de menaces et sensibiliser les employés à l'évolution de ces menaces.
- Bloquer le téléchargement ou la duplication d'un fort volume d'informations sans autorisation préalable.
- Limiter les droits de modification des filtres antipourriel et empêcher le déblocage des applications et plugiciels.

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › SÉCURISATION DES POINTS D'ENTRÉE

### PÉRIPHÉRIQUES MALVEILLANTS

Retour à l'autodiagnostic

Les périphériques amovibles (clé USB souris et clavier) font désormais partie de l'environnement technologique. Une connexion filaire ou Bluetooth est nécessaire pour activer ces périphériques.

Même si l'apparence d'un périphérique semble anodine, il est possible qu'il renferme un dispositif malveillant (ex. : adapteur Wi-Fi USB ou un logiciel malveillant dans le connecteur USB d'un clavier).

### BONNES PRATIQUES

> Ne pas brancher de périphériques amovibles dont la source n'est pas connue, comme des clés USB remises lors d'événements ou des souris trouvées.

> Désactiver la recherche automatique de nouvelles connexions des périphériques, notamment le Bluetooth.

> Désactiver le branchement automatique d'un nouveau périphérique et configurer manuellement le branchement des périphériques connus.

> Partager les meilleures pratiques avec toutes les personnes qui utilisent les appareils professionnels ou qui sont connectées au même réseau, comme les autres occupants de la résidence.

> Prêter attention aux réseaux sans-fil intégrés dans les voitures louées : les données ne sont pas automatiquement effacées lorsque la voiture est rendue au locateur.

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › SÉCURISATION DES POINTS D'ENTRÉE

### ÉVALUATION DES VULNÉRABILITÉS

Retour à l'autodiagnostic

Lorsqu'une organisation met en place les mesures de sécurité qu'elle considère raisonnables, son exposition au risque diminue mais n'est pas nulle ni stable pour autant. Une évaluation des vulnérabilités par un spécialiste de la sécurité de l'information devrait donc être effectuée à intervalle régulier. Pareille mesure sert à évaluer la capacité d'un système à bloquer des tentatives de piratage selon un degré variable de complexité, et à documenter les vulnérabilités découvertes afin d'y remédier.

**BONNES PRATIQUES**

- Procéder régulièrement à des tests d'intrusion logique (sécurité des systèmes, simulation d'hameçonnage, etc.).
- Procéder à l'occasion à des tests d'intrusion physique (entrée dans les lieux de travail, les salles de photocopie, de courrier et de serveurs, etc.).
- Procéder à des tests de piratage psychologique (obtention de renseignements utiles tels des mots de passe, installation d'un logiciel exécutée par un courriel, personnification d'un dirigeant pour effectuer un virement urgent, etc.).

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › SÉCURISATION DES POINTS D'ENTRÉE

### GESTION DES MISES À JOUR

Retour à l'autodiagnostic

Les mises à jour corrigent les vulnérabilités des logiciels et assurent l'actualisation des applications matérielles (équipements informatiques) et logicielles du système informatique de l'organisation.

Si les mises à jour automatiques sont indiquées pour les logiciels de sécurité (pare-feu, antivirus, etc.), il est cependant préférable, pour les autres types de logiciels, de procéder à des vérifications préalables pour s'assurer que les mises à jour sont compatibles avec le système en place. Dans le cas des grands éditeurs de logiciels, les mises à jour problématiques sont rares et généralement rapidement corrigées. Dans les autres cas, il peut être plus fréquent qu'une mise à jour nécessite une correction et qu'il faille contacter l'éditeur.

#### BONNES PRATIQUES

- Conserver un inventaire des applications matérielles et logicielles utilisées dans l'organisation et de leurs mises à jour.
- Dans la mesure du possible, configurer les applications pour que les mises à jour disponibles soient portées à l'attention de l'administrateur réseau et non installées automatiquement.
- Les applications de sécurité qui assurent la surveillance des signatures des codes malveillants ou des virus doivent toutefois être configurées pour être mises à jour automatiquement afin de pallier rapidement aux nouvelles vulnérabilités.
- Pour les applications névralgiques, procéder à des tests en environnement (autre qu'en production) afin de s'assurer de la compatibilité des mises à jour avant la mise en production.

3

# SÉCURITÉ DE L'ENVIRONNEMENT

## › SÉCURISATION DES POINTS D'ENTRÉE

### SURVEILLANCE ET GESTION DES ALERTES

La surveillance du périmètre de sécurité et des systèmes internes est assurée par des outils logiciels qui détectent les situations anormales, par exemple les tentatives d'intrusion en provenance d'emplacements douteux. Les données colligées dans les journaux ou les paramètres de configuration des outils de protection du réseau sont alors comparés à des normes de référence. Le cas échéant, une alerte signale la présence d'un problème potentiel.

**BONNES PRATIQUES**

> Connaître le fonctionnement des alertes dans les systèmes utilisés.

> S'assurer que les personnes chargées de donner suite aux alertes lorsqu'elles sont générées ont les compétences et l'autonomie nécessaires pour ce faire.

> Documenter ou autrement garder trace des alertes et des mesures de suivi afin, d'une part, de démontrer la diligence de l'organisation en matière de sécurité de l'information et, d'autre part, de détecter des tendances à plus long terme.

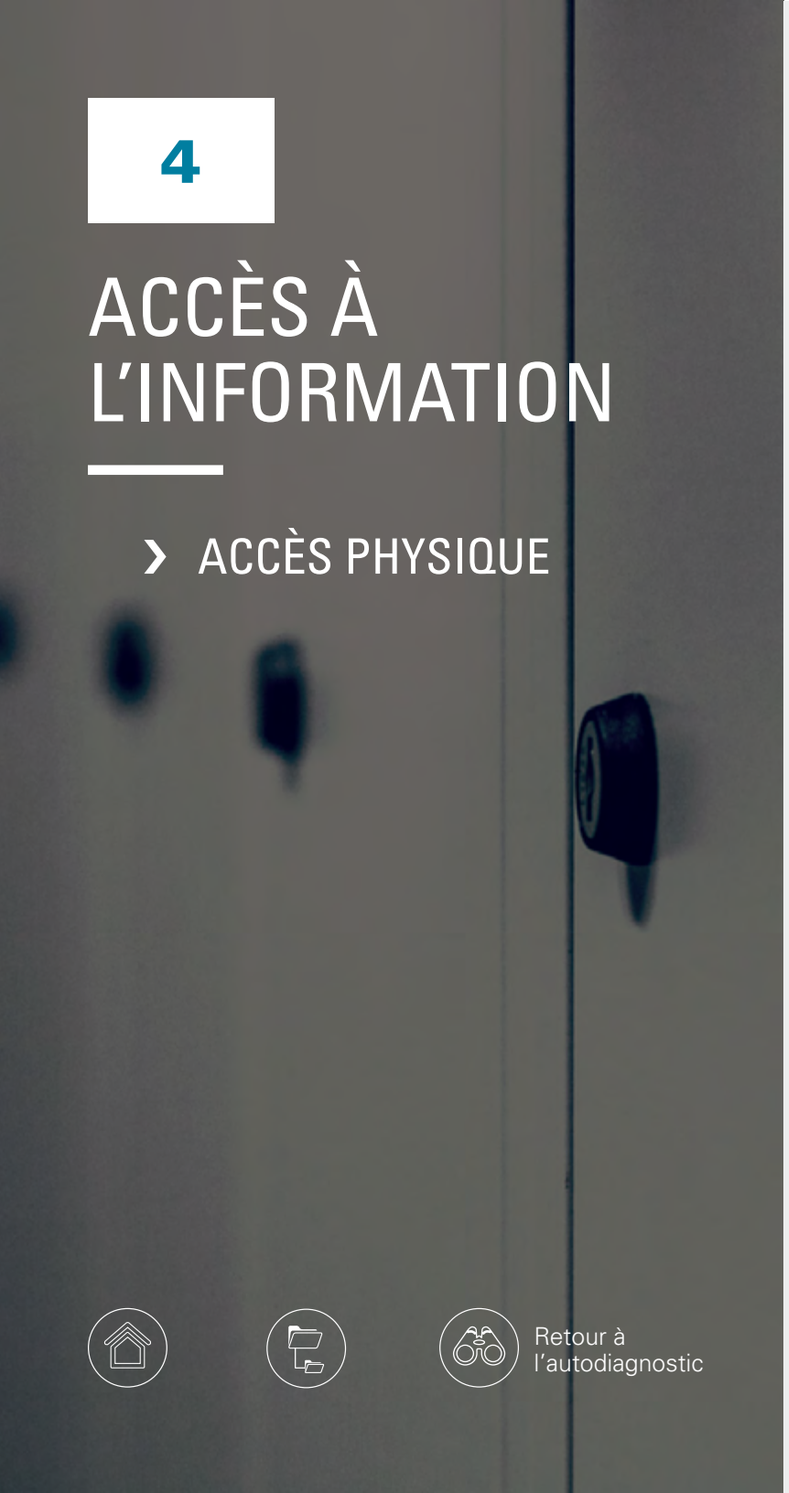
Retour à l'autodiagnostic

4

# ACCÈS À L'INFORMATION

| | | |
|---|---|---|
| ACCÈS PHYSIQUE | ACCÈS LOGIQUE | MOTS DE PASSE |
| GESTIONNAIRE DE MOTS DE PASSE | AUTRES MÉTHODES D'AUTHENTIFICATION | |

Retour à l'autodiagnostic



4

# ACCÈS À L'INFORMATION

## › ACCÈS PHYSIQUE

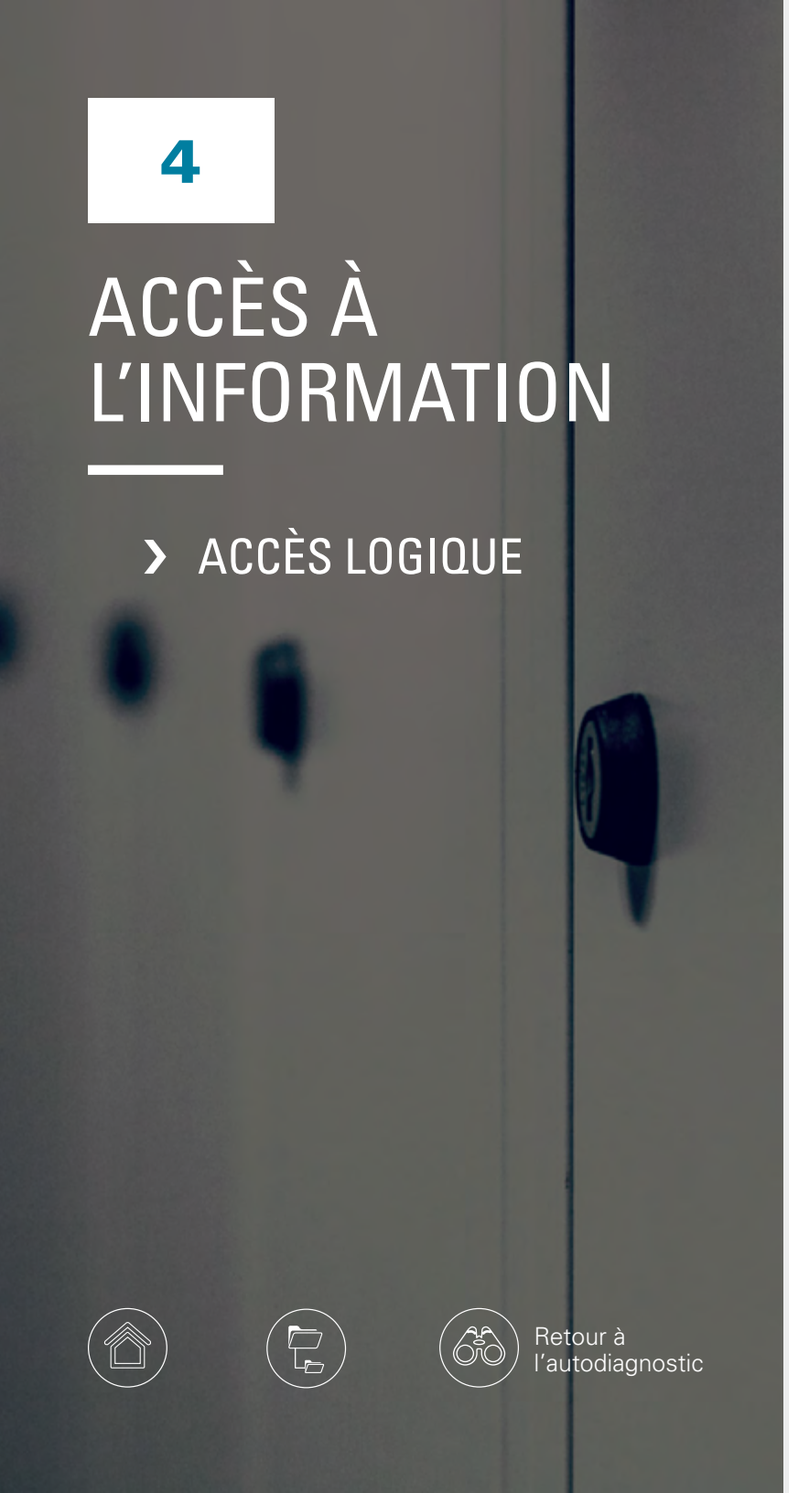
Pour limiter les risques que quelqu'un entende, voie ou prenne physiquement possession d'informations confidentielles, l'accès physique aux locaux d'une organisation doit être sécurisé – salles de réunion ou de consultation, de courrier, d'impression et de serveurs, bureaux, etc.

La popularité du télétravail fait évoluer le concept de bureau et de périmètre à protéger. Le domicile, la voiture personnelle, les transports en commun et les cafés sont autant d'endroits où on peut accéder à des informations confidentielles et où les risques d'espionnage par-dessus l'épaule sont accrus.

### BONNES PRATIQUES

- Fermer les bureaux et les locaux à clé.
- Assurer la gestion des clés et des clés magnétiques en circulation.
- Ne pas conserver les clés magnétiques avec une carte professionnelle ou toute autre indication du lieu de travail.
- S'assurer que la perte ou le vol de cartes magnétiques soit rapporté de toute urgence au responsable désigné.
- Munir les écrans utilisés dans un environnement auquel des tiers ont accès de filtres protecteurs polarisés (écrans de confidentialité) afin d'en limiter l'angle de vision.
- Contrôler l'accès des clients et des visiteurs et les accompagner dans les espaces de travail.
- Accompagner tout client ou visiteur dans les salles de serveurs et journaliser les accès à ces lieux (entrées et sorties).
- Tenir un registre général des entrées et sorties des clients et visiteurs.
- Veiller à ce que le personnel ne laisse aucun document confidentiel ou sensible à la vue de tous (imprimante, table de travail, etc.), tant dans les locaux de l'organisation qu'au domicile, dans les transports en commun ou dans les espaces publics ou partagés et considérer l'implantation d'une politique du bureau propre et de l'écran vide.
- Prévoir une pièce privée pour discuter avec un client/un collègue d'informations sensibles, que ce soit au bureau ou au domicile.
- S'assurer que le personnel applique les mesures de contrôle.

Retour à l'autodiagnostic



4

# ACCÈS À L'INFORMATION

## › ACCÈS LOGIQUE

De la même façon que l'accès physique, il est possible de limiter et de sécuriser les points d'accès logique aux données.

### BONNES PRATIQUES

> Éviter d'utiliser des réseaux non sécurisés, notamment dans les lieux publics, et privilégier les outils de sécurisation des connexions mis en place par l'organisation.

> Conserver les documents dans un emplacement centralisé (système de gestion des documents électroniques, serveurs de fichiers, etc.).

> Inciter les employés à conserver les documents le moins longtemps possible sur leurs ordinateurs ou autres appareils portatifs.

> Mettre en place des mesures d'accès à distance aux données et aux applications (ex. : un réseau privé virtuel (VPN), une passerelle Citrix ou d'autres technologies au même effet).

> Programmer son ordinateur pour qu'il se mette en veille automatique après un certain laps de temps.

> Mettre à la disposition des visiteurs un réseau distinct de celui donnant accès aux données.

> Mettre en place une procédure applicable lors du départ d'un employé et prévoyant :

- la désactivation de ses accès, par exemple en changeant les mots de passe puis, éventuellement, en les supprimant, donnant ainsi à l'organisation le temps de recevoir les courriels des clients adressés à l'ancien employé et de procéder à des suivis;
- l'archivage des documents de l'ancien employé (y compris les courriels et le calendrier).

Retour à l'autodiagnostic

4

# ACCÈS À L'INFORMATION

## › MOTS DE PASSE

L'authentification est la façon pour une personne ou un système de vérifier l'identité de l'utilisateur. Pour jouer efficacement son rôle, le mot de passe doit être robuste et tenu secret. Si un site Web est victime d'une brèche de sécurité et que des mots de passe sont divulgués, ils peuvent être utilisés pour tenter d'infiltrer d'autres sites ou systèmes.

### BONNES PRATIQUES

- Ne pas utiliser le même mot de passe pour plus d'un système ou site Web, particulièrement les sites où circule de l'information sensible, comme les services courriels ou les plateformes bancaires.
- Ne pas utiliser une adresse courriel professionnelle pour s'inscrire à des sites ou applications à des fins personnelles (ex. : Facebook, Uber, DoorDash, etc.).
- Changer vos mots de passe régulièrement et en cas de compromission suspectée (des changements trop fréquents incitent toutefois l'utilisateur à former des mots de passe aussi simples que possible). Un mot de passe devrait être changé au moins aux trois mois et ne pas être réutilisé avant deux ans.
- Ne pas utiliser des dates, des renseignements personnels ou des mots du dictionnaire.
- Privilégier la constitution de mots de passe à l'aide de phrases dont seule la première lettre de chaque mot est conservée, avec des insertions de chiffres et de symboles.
- Utiliser un gestionnaire de mots de passe.
- Changer les noms d'utilisateur et les mots de passe par défaut, surtout pour les comptes administrateurs (par exemple, sur le routeur de l'organisation, une cible de choix pour les pirates).
- Limiter, si le système le permet, le nombre de tentatives infructueuses afin de bloquer l'accès.
- Prévoir un processus d'authentification par lequel un utilisateur peut réinitialiser un mot de passe oublié.
- Gérer les comptes utilisateurs (création, suspension, destruction, accès spéciaux) afin de limiter les accès aux personnes autorisées.
- Gérer les droits d'accès par profil, selon les tâches et fonctions des postes de l'organisation plutôt que par individu, et les réviser périodiquement.
- S'assurer que les employés ayant des accès privilégiés utilisent des noms d'utilisateur distincts dans leurs tâches quotidiennes et dans leur rôle d'administrateur.
- Limiter, journaliser et analyser l'accès aux actifs informationnels critiques.
- Conserver son nom d'utilisateur et son mot de passe dans un endroit accessible à un collègue qui pourra ouvrir l'ordinateur en cas de décès ou d'incapacité subite de son utilisateur habituel. Ne pas partager ces informations en cas d'absence ou de congé.
- Ne jamais partager son mot de passe, pour quelque raison que ce soit. Si plusieurs accès sont nécessaires, configurer des accès distincts, pour en garder la trace

Retour à l'autodiagnostic

4

# ACCÈS À L'INFORMATION

## › GESTIONNAIRE DE MOTS DE PASSE

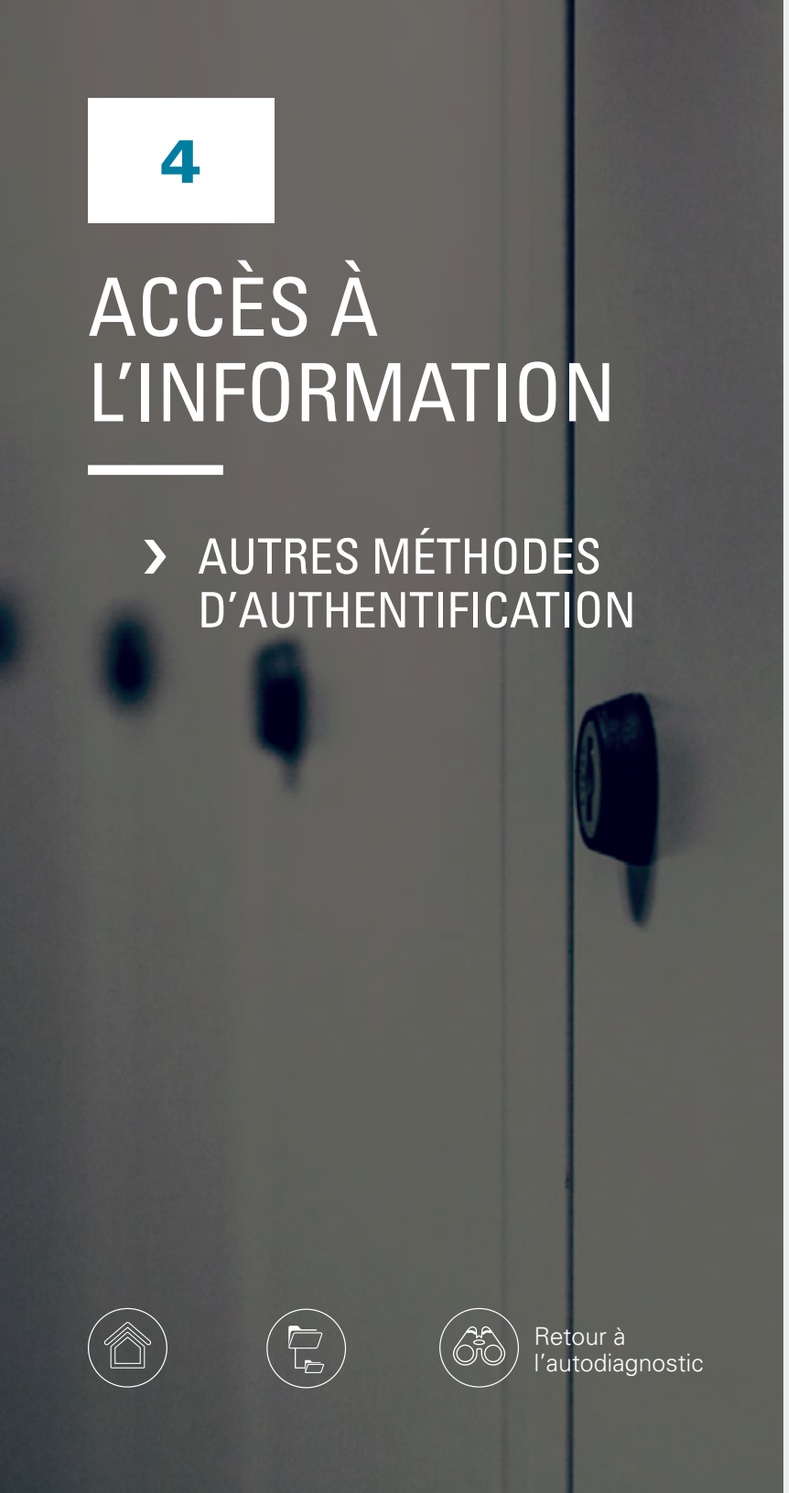
Un gestionnaire de mots de passe est une base de données qui renferme tous les identifiants d'un utilisateur (nom d'utilisateur, mots de passe, réponses aux questions secrètes, etc.). Cette base de données est chiffrée et elle-même protégée par un mot de passe le plus complexe possible. Certains gestionnaires sont basés sur le Web, alors que d'autres sont des applications qui génèrent un fichier local. Le gestionnaire de mots de passe peut générer des mots de passe aléatoirement, et le fait que l'on n'ait plus besoin de s'en souvenir favorise l'utilisation de très longs mots de passe, différents pour chaque compte, et leur changement fréquent.

### BONNES PRATIQUES

> Utiliser un gestionnaire de mots de passe.

> Compte tenu de l'importance du mot de passe maître, avoir un moyen sécuritaire pour le récupérer en cas de besoin.

Retour à l'autodiagnostic



4

# ACCÈS À L'INFORMATION

## › AUTRES MÉTHODES D'AUTHENTIFICATION

Dans certains cas, il peut être souhaitable de renforcer l'accès logique à un système en utilisant deux facteurs d'authentification. Par exemple, pour accéder à distance au réseau de l'organisation, via le serveur gérant le réseau privé virtuel ou un serveur hébergeant de l'information critique.

Des jetons physiques, affichant un code changeant fréquemment, ou un message texte envoyé lors du processus d'authentification peuvent constituer un second facteur d'authentification, en plus du mot de passe.

La biométrie est également un moyen d'authentification gagnant en popularité sur certains modèles d'ordinateurs portatifs et téléphones cellulaires. Les risques (notamment ceux relatifs à la vie privée) sont diminués lorsque les informations sont stockées seulement sur l'appareil et chiffrées et qu'elles font l'objet d'une transformation à sens unique afin qu'il soit impossible de recréer, par exemple, l'empreinte digitale à partir de l'information enregistrée.

### BONNES PRATIQUES

> Activer l'authentification à deux facteurs sur les systèmes lorsque l'option est supportée (notamment pour les réseaux privés virtuels) et bloquer sa désactivation par le personnel non autorisé.

> Privilégier l'utilisation de mesures biométriques (principalement les empreintes digitales) comme authentifiant.

Retour à l'autodiagnostic

5

# DISPOSITION ET RÉAFFECTATION DE MATÉRIEL

Retour à l'autodiagnostic

Lorsqu'on dispose d'un appareil ou d'un support informatique, il ne doit pas y subsister d'information pour éviter toute brèche du périmètre de sécurité de l'organisation.

Lorsqu'un appareil informatique ou un support d'information est réaffecté à autre employé, donné à un organisme de bienfaisance ou remis à son locateur (tel qu'une imprimante multifonction qui comporte un disque dur dont la mémoire interne peut encore contenir de l'information confidentielle), l'information doit en être détruite au préalable. Le simple formatage est insuffisant puisque l'information peut être récupérable.

## BONNES PRATIQUES

- Utiliser les outils logiciels appropriés pour la destruction de l'information.
- La réinitialisation des téléphones et des tablettes peut être une méthode suffisante, mais l'évolution rapide des méthodes et des outils de recouvrement des données pourrait nécessiter de nouvelles mesures pour s'assurer de la destruction des données.
- Détruire soi-même l'information contenue sur un support avant de s'en départir. Des outils logiciels simples d'utilisation permettant de détruire l'information stockée sur un support sont offerts sur le marché. On peut également recourir à un fournisseur de services de destruction sécuritaire.
- En ce qui concerne les appareils loués, s'assurer que le locateur procède à la destruction de l'information contenue sur les disques durs ou l'effectuer soi-même si on y est autorisé.
- Reprendre le matériel informatique et réaffecter les comptes (LinkedIn, Facebook, Twitter) appartenant à l'organisation au départ d'un employé.

6

# SÉCURITÉ APPLICATIVE ET COMMUNICATIONS

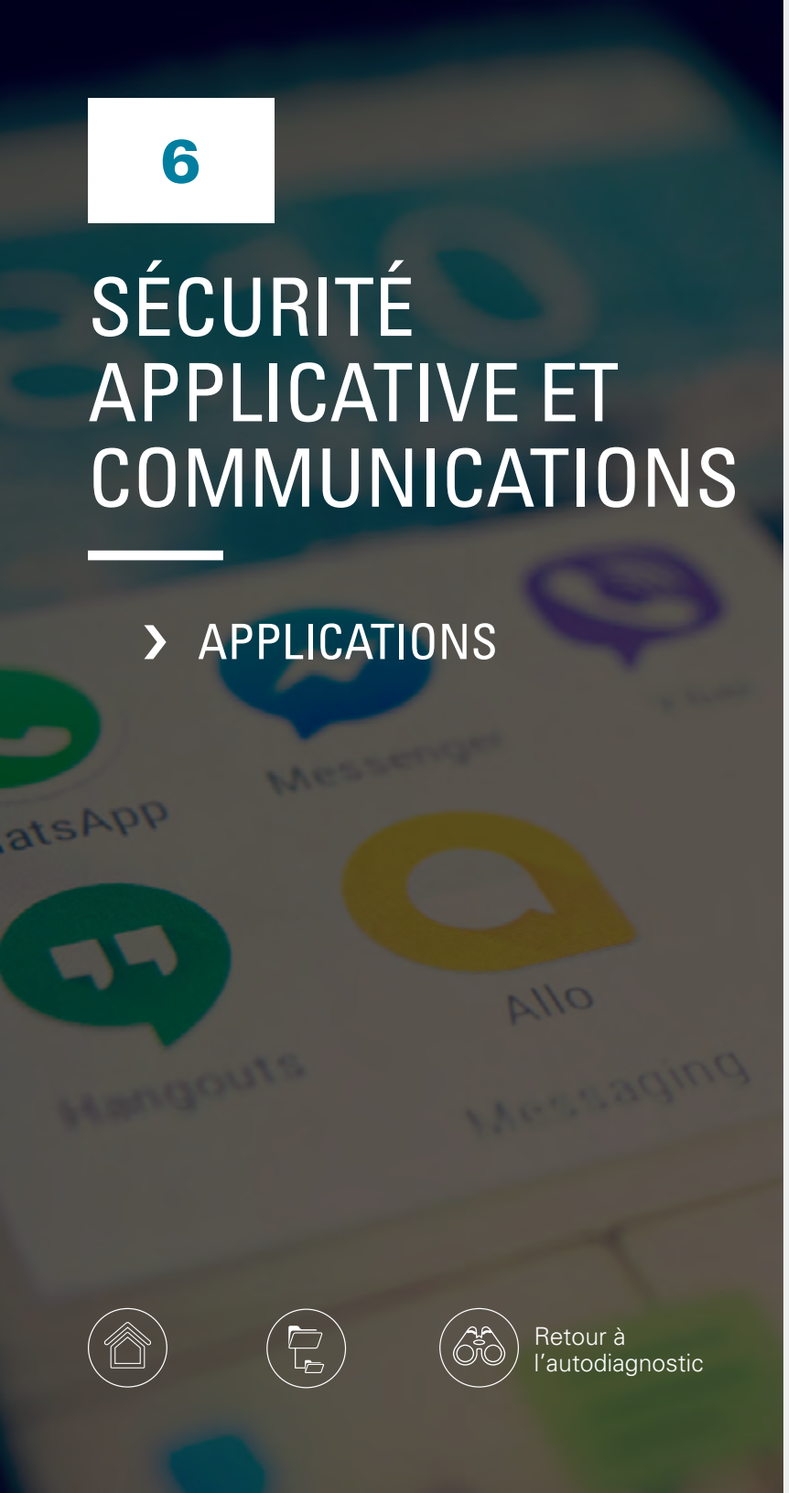
APPLICATIONS

COURRIEL

MESSAGERIE INSTANTANÉE

OUTILS COLLABORATIFS

Retour à l'autodiagnostic




6

# SÉCURITÉ APPLICATIVE ET COMMUNICATIONS

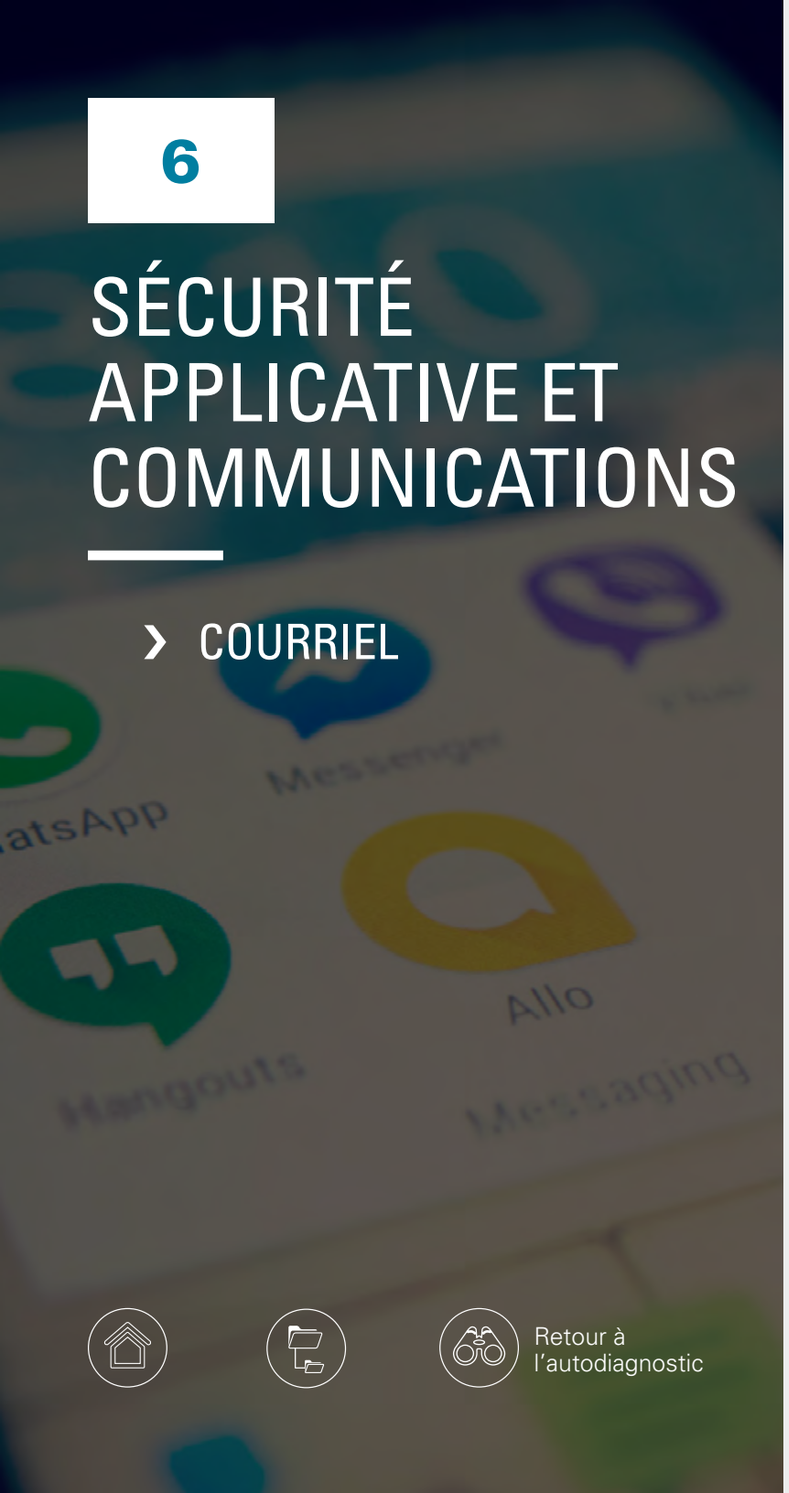
## › APPLICATIONS

Les applications servent à la collecte, au traitement et à la communication de l'information. Elles ont souvent accès à un large éventail d'informations (contacts, courriels, géolocalisation, documents sur l'appareil) et se retrouvent le plus souvent sur les ordinateurs, les serveurs, les tablettes, les téléphones, l'infonuage, mais peuvent également se retrouver sur les téléviseurs, dans les caméras de sécurité, dans les montres intelligentes ou dans tout autre objet connecté.

### BONNES PRATIQUES

- Comprendre le fonctionnement de ces applications et ce à quoi elles ont accès.
- Considérer la ségrégation des données personnelles et professionnelles sur les ordinateurs et appareils mobiles. Bien que cette pratique complexifie leur utilisation (alternance entre deux profils distincts, utilisation de diverses applications), elle assure la protection des données professionnelles et une utilisation plus « libre » de l'appareil à des fins personnelles.
- Lire les politiques de protection des renseignements personnels et de sécurité de l'information (incluant la confidentialité) et le contrat de licence d'utilisateur final (CLUF) des applications installées et en comprendre le fonctionnement quant à la circulation des informations qu'elles traitent.
- Privilégier les applications des appareils mobiles qui hébergent les données sur les serveurs de l'organisation plutôt que sur l'appareil ou, à défaut, sur des serveurs en infonuagique en sol canadien.
- Procéder à la mise à jour des applications dès qu'une nouvelle version est disponible.
- Limiter aux personnes autorisées l'installation d'applications sur les appareils.

Retour à l'autodiagnostic




6

# SÉCURITÉ APPLICATIVE ET COMMUNICATIONS

## › COURRIEL

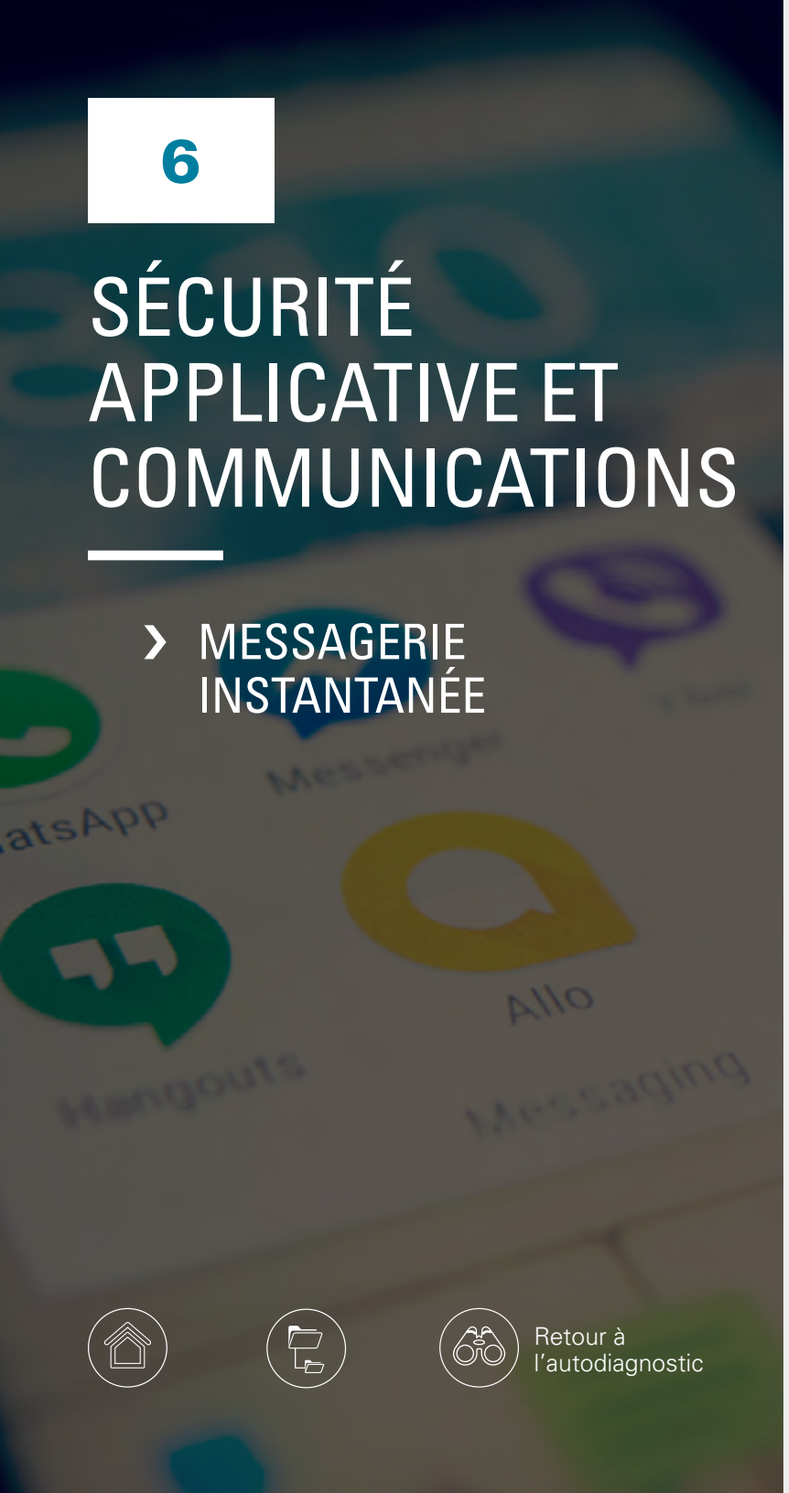
Sans chiffrement, le courriel n'assure pas la confidentialité des informations échangées.

Parmi les risques reliés au courriel, on relève l'interception de messages envoyés en clair, l'usurpation d'identité, la fraude, le piratage psychologique, l'ingénierie sociale (courriel d'un prétendu président à un contrôleur des finances pour autoriser un paiement d'urgence) et la cybercriminalité (rançongiciels, virus ou code malveillant).

### BONNES PRATIQUES

- Assurer la formation du personnel contre les arnaques par courriel (hameçonnage, etc.).
- Retenir les services d'une firme de sécurité de l'information et procéder à l'occasion à des tests de piratage psychologique.
- Établir des procédures d'authentification des tiers avant de libérer des paiements ou de communiquer des renseignements sensibles.
- Protéger les pièces jointes par un mot de passe qui sera transmis par un autre moyen de communication, ou utiliser une plateforme de livraison sécurisée.
- Vérifier les conditions d'utilisation du service de messagerie pour s'assurer que le prestataire de services n'a pas le droit d'utiliser le contenu à quelque fin que ce soit.
- Éviter les services de messagerie dont les serveurs ne sont pas localisés au Canada ou qui appartiennent à une société étrangère.
- Conserver une copie de sauvegarde des courriels.
- Convenir avec le client de l'utilisation des courriels comme mode de communication et obtenir le consentement exprès du client dans le cas où des documents couverts par le secret professionnel seraient transmis.
- Programmer un message d'absence automatique pour informer l'expéditeur de son incapacité à lire les messages sans toutefois donner des détails superflus que d'éventuels fraudeurs pourraient utiliser.
- Programmer l'affichage d'un avertissement dans tous les courriels de source externe invitant le destinataire à bien examiner les liens et les pièces jointes.

Retour à l'autodiagnostic




6

# SÉCURITÉ APPLICATIVE ET COMMUNICATIONS

## › MESSAGERIE INSTANTANÉE

La messagerie instantanée peut remplacer le courriel. Si elle n'est utilisée qu'à l'interne, les risques sont les mêmes que ceux de toute application. Si elle est également utilisée pour communiquer avec la clientèle, elle devient alors un point d'entrée supplémentaire qu'il convient de sécuriser. Dans tous les cas, cette application comporte des risques liés au chiffrement des données en transit et au repos, à la localisation des serveurs (au Canada ou à l'extérieur) et à la propriété de l'éditeur de l'application (canadien ou étranger).

### BONNES PRATIQUES

- Comprendre le fonctionnement de l'application.
- Sécuriser l'application si elle est utilisée pour communiquer à l'extérieur du réseau de l'organisation.
- Vérifier les conditions d'utilisation du service de messagerie pour s'assurer que le prestataire de services n'a pas le droit d'utiliser le contenu à quelque fin que ce soit.
- Éviter les services de messagerie dont les serveurs ne sont pas localisés au Canada ou qui appartiennent à une société étrangère.

Retour à l'autodiagnostic


6

# SÉCURITÉ APPLICATIVE ET COMMUNICATIONS

## › OUTILS COLLABORATIFS

Les outils collaboratifs font partie du quotidien de bon nombre de travailleurs. Ils facilitent les échanges entre collègues à l'interne et peuvent aussi ouvrir la voie à des collaborateurs externes ou occasionnels. Ils donnent plus d'autonomie aux équipes de travail, qui dès lors sollicitent moins les spécialistes des TI. En contrepartie, cette autonomie augmente les risques de bris de sécurité.

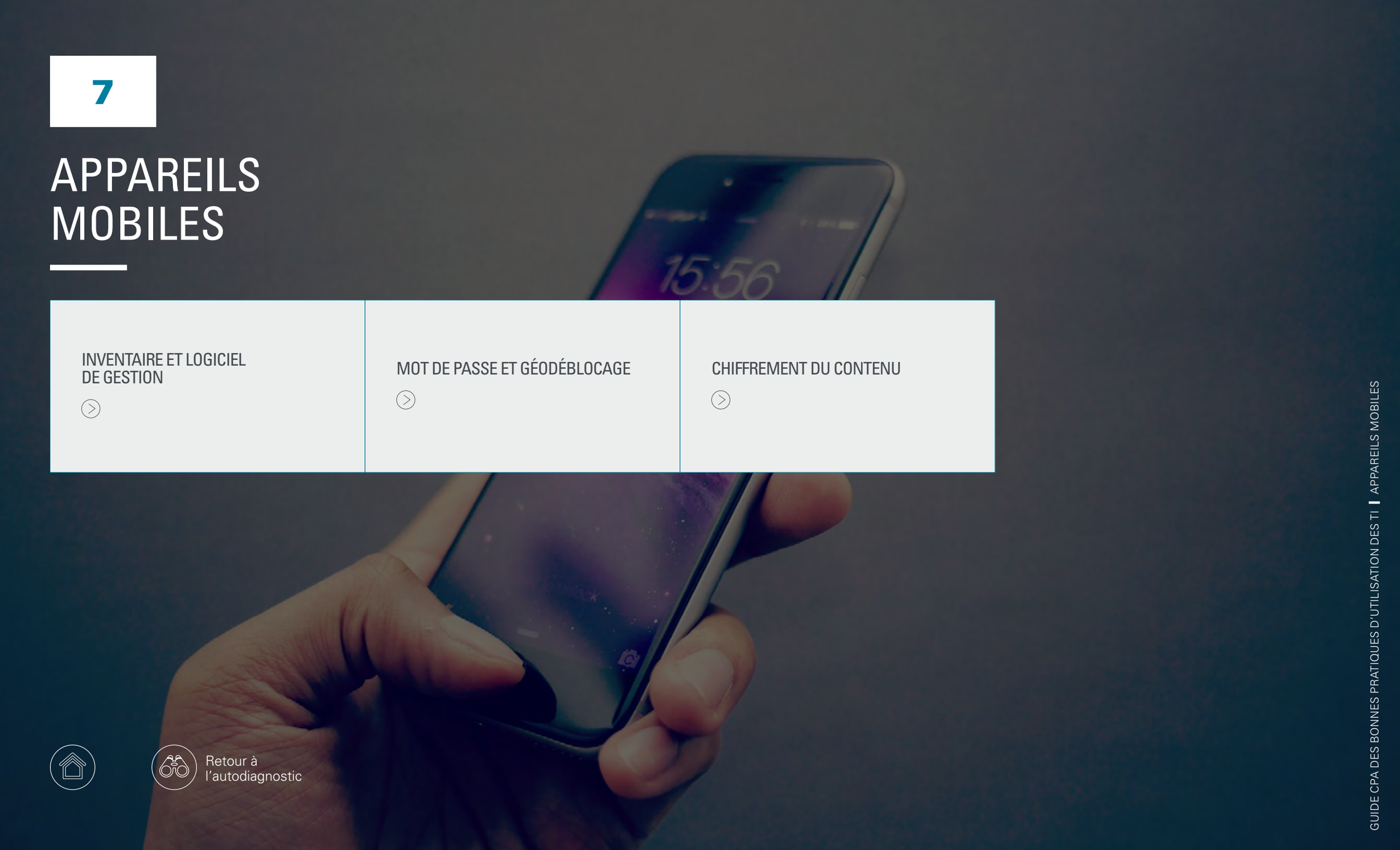
### BONNES PRATIQUES

- Encadrer ou limiter les droits de partage.
- Privilégier la création de liens individualisés plutôt que d'utiliser un lien unique pour partager des informations à un groupe de personnes.
- Encadrer le partage d'informations par clavardage.
- Configurer l'effacement automatique des discussions en ligne dans un délai déterminé.
- Catégoriser les informations et les utilisateurs selon la nature de leur rôle.
- Tenir à jour en continu le registre des employés et des collaborateurs externes ayant accès aux documents et retirer les accès lorsqu'une personne n'en a plus besoin ou au terme d'une période définie par défaut.

Retour à l'autodiagnostic

7

# APPAREILS MOBILES



| | | |
|---|---|---|
| INVENTAIRE ET LOGICIEL DE GESTION | MOT DE PASSE ET GÉODÉBLOCAGE | CHIFFREMENT DU CONTENU |

Retour à l'autodiagnostic

7

# APPAREILS MOBILES

## › INVENTAIRE ET LOGICIEL DE GESTION

Retour à l'autodiagnostic

Il est important de conserver un inventaire des appareils mobiles de façon à consigner les pertes et les vols et à assurer la gestion des incidents.

Les logiciels de gestion (ou gestion de terminaux mobiles) contribuent également à sécuriser les appareils mobiles en permettant la mise à jour des applications ou du système d'exploitation et la prise de contrôle des appareils à distance. Cette fonction est particulièrement utile pour détruire l'information à distance en cas de perte ou de vol d'un appareil mobile ou, à l'inverse, pour procéder automatiquement à la sauvegarde des données. Dans la mesure où les données accessibles sur l'appareil mobile sont transitoires (les données originelles sont conservées ailleurs ou une copie de sauvegarde est conservée), il n'y a pas de risque de détruire des informations uniques.

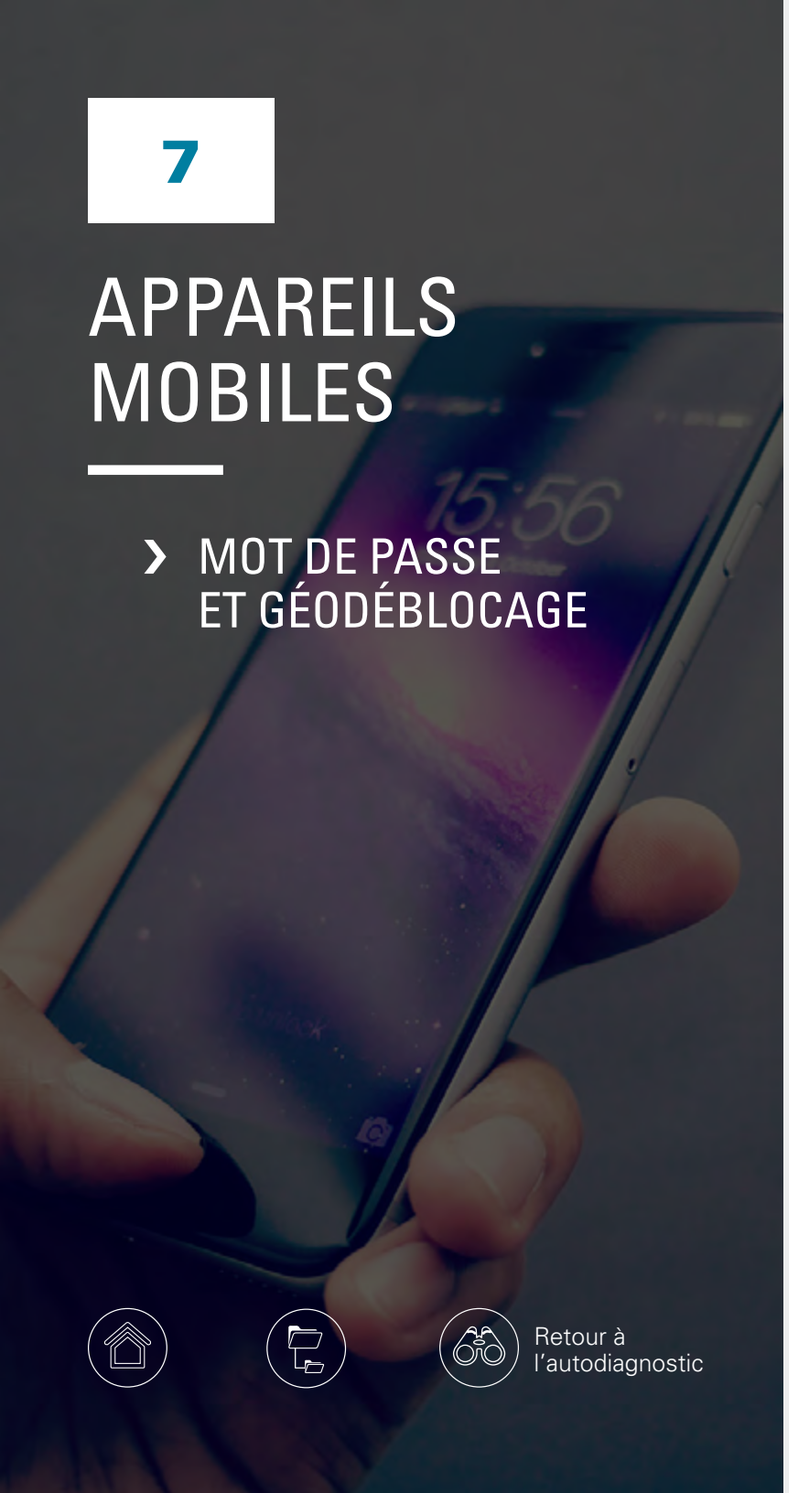
### BONNES PRATIQUES

- Se munir d'un logiciel de gestion des appareils mobiles.
- Inclure dans l'inventaire les identifiants usuels (modèle, numéro de série), la version du système d'exploitation, l'état du chiffrement, la version du logiciel de gestion de l'appareil mobile et le nom de l'utilisateur et gérer l'inventaire au moyen du logiciel de gestion ou, à défaut, manuellement.
- Adopter une politique de sécurisation des appareils mobiles (ex. : interdiction de les laisser dans une voiture) et de divulgation des vols d'appareils mobiles professionnels ou d'appareils mobiles personnels utilisés à des fins professionnelles.
- Sauvegarder les données des appareils suivant un calendrier de sauvegarde établi en fonction du type de données.
- Effacer les données à distance lorsque nécessaire.

7

# APPAREILS MOBILES

## › MOT DE PASSE ET GÉODÉBLOCAGE

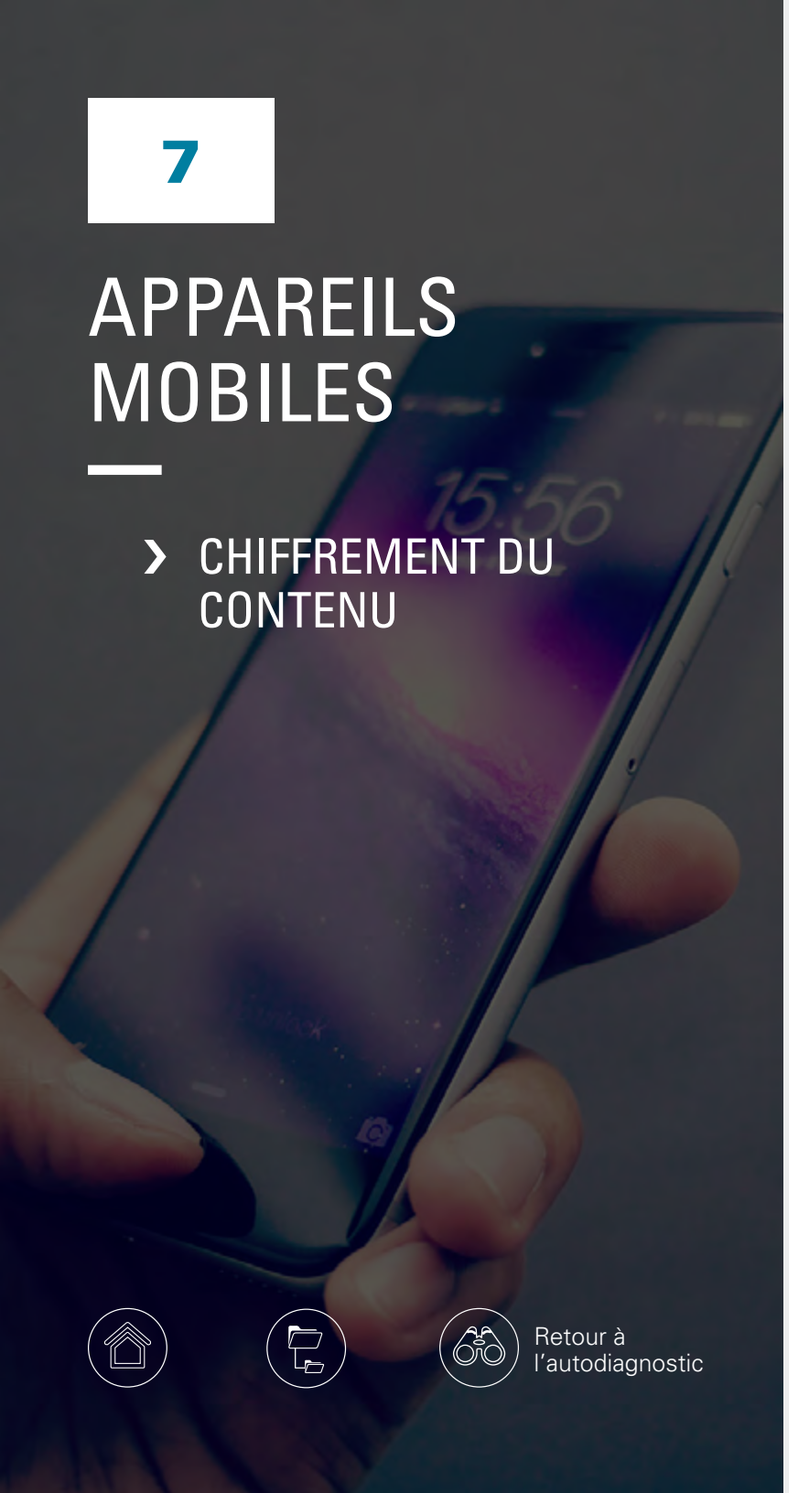


Retour à l'autodiagnostic

Les exigences relatives aux mots de passe pour les appareils mobiles sont souvent perçues comme des irritants : la longueur et les caractères spéciaux ne sont pas adaptés aux écrans tactiles et il faut les saisir fréquemment. La tentation est donc forte de déverrouiller automatiquement l'appareil selon sa géolocalisation (GPS) ou s'il est connecté à un réseau spécifique. Cette pratique comporte le risque de perdre le contrôle d'un appareil qui se serait automatiquement déverrouillé lors de sa connexion, par exemple en l'oubliant dans une salle de conférence accessible au public.

### BONNES PRATIQUES

- S'assurer de la sécurité du périmètre physique, c'est-à-dire ne pas activer le géodéblocage dans un environnement que l'on ne contrôle pas (par opposition à une maison ou un bureau non accessible au public).
- N'activer le géodéblocage qu'une fois le mot de passe entré.
- Réactiver le blocage dès qu'on sort de l'environnement contrôlé.



7

# APPAREILS MOBILES

## › CHIFFREMENT DU CONTENU

Retour à l'autodiagnostic

Les appareils mobiles de tous types, y compris les ordinateurs portables, offrent l'option de chiffrer le contenu. Le contenu n'est alors accessible qu'une fois l'utilisateur correctement authentifié. Le processus est transparent pour l'utilisateur et limite grandement les risques d'atteinte à la confidentialité si l'appareil devait être perdu. Puisque ces options sont offertes à un coût très accessible (voire gratuitement avec certains appareils), il serait déraisonnable de s'en priver. Il importe de protéger et de ne pas perdre la clé de déchiffrement.

### BONNES PRATIQUES

> Configurer le chiffrement automatique sur les appareils mobiles en activant la fonction ou en acquérant l'application.

> Sécuriser les clés de déchiffrement en fonction du mode de gestion du chiffrement. Dans le cas où le chiffrement est géré de façon centralisée, une solution logicielle peut assurer la sécurité des clés. La clé de déchiffrement peut également être placée dans un endroit sécuritaire, tel un coffret de sûreté. Si le chiffrement est géré par l'appareil et activé par l'utilisateur au moyen d'un mot de passe, celui-ci doit être protégé.

8

# ENCADREMENT DES APPAREILS *AVEC* (apportez votre équipement personnel de communication)

Retour à l'autodiagnostic

De nombreuses organisations donnent accès à certaines de leurs données et applications, notamment au courriel, sur les appareils mobiles de leurs employés. Cette situation a des répercussions de part et d'autre.

Alors que l'employé voit la frontière de sa vie privée devenir plus floue, l'employeur subit une perte partielle de contrôle de ses données. Ainsi, l'employé donne à son employeur la possibilité d'accéder au contenu de son appareil (registre d'appels, messagerie texte, etc.) et de détruire ses données à distance. De son côté, l'employeur voit ses données confidentielles circuler dans un environnement poreux. Pour limiter ces risques, il convient de recréer des frontières entre les données personnelles et les données professionnelles.

## BONNES PRATIQUES

> Mettre en place une politique relative à l'utilisation d'appareils personnels dans un contexte professionnel. Cette politique doit :
  - réitérer la propriété des actifs informationnels de l'organisation;
  - clarifier l'expectative de vie privée de l'utilisateur par rapport au droit de l'employeur de vérifier l'utilisation faite de ses ressources informationnelles et de mener des enquêtes;
  - préciser si un logiciel de gestion des appareils mobiles sera installé sur l'appareil et s'il sera possible de détruire de l'information à distance dans le cas d'un incident de sécurité le requérant;
  - exiger l'instauration et le maintien à jour de mesures de sécurité de base, notamment un antivirus.
> Considérer la perte ou le vol d'un appareil *AVEC* comme un incident de sécurité et prévoir un numéro de téléphone d'urgence ou un portail Web pour rapporter ce type d'incident.
> Sensibiliser les employés à la politique et obtenir leur adhésion.
> Utiliser des appareils distincts pour les besoins d'affaires (courriels, contacts, téléphones, documents) ou des applications qui permettent une telle ségrégation.
> Limiter la conservation des données professionnelles sur les appareils *AVEC* et les verser dans l'environnement principal dès que possible afin que les données professionnelles sur les appareils mobiles ne soient pas les copies principales et uniques.

9

# COMMUNICATION DE DOCUMENTS

| MÉTADONNÉES | COMMUNICATION SÉCURISÉE | EXTRANET |
| --- | --- | --- |

9

# COMMUNICATION DE DOCUMENTS

## › MÉTADONNÉES

Retour à l'autodiagnostic

Les documents informatiques sont constitués des données elles-mêmes et des métadonnées. Les métadonnées renseignent notamment sur le contexte du document : la date de création, les auteurs, le nom du dossier, le chemin d'accès dans l'architecture du réseau, etc. La divulgation de certaines de ces informations peut compromettre le secret professionnel, par exemple lorsque des documents créés pour un client sont utilisés comme modèle pour un mandat subséquent. La plupart des logiciels permettent de nettoyer aisément les métadonnées.

### BONNES PRATIQUES

> Nettoyer les métadonnées avant l'utilisation et la communication de documents à des tiers ou à des clients.

> Encadrer la transmission de documents à l'externe par les utilisateurs habilités.

9

# COMMUNICATION DE DOCUMENTS

## › COMMUNICATION SÉCURISÉE

Retour à l'autodiagnostic

Les messages envoyés par courriel et leurs pièces jointes ne sont pas, par défaut, confidentiels. Leur contenu est transmis « en clair », ce qui signifie qu'ils sont librement lisibles par quiconque y a accès, légitimement ou non : un intermédiaire technique, l'hébergeur du courriel Web gratuit, une agence de renseignement, un gouvernement étranger ou un pirate informatique, par exemple. Le contenu d'un message (le corps du texte ainsi que les pièces jointes) peut être chiffré. Il n'est toutefois pas possible de chiffrer les entêtes du message (date, sujet, nom et adresse de l'expéditeur et des destinataires, etc.).

Afin de préserver la confidentialité de leurs échanges, le CPA et son client peuvent convenir d'une plateforme de communication sécurisée. Le message et sa pièce jointe y sont d'abord versés par l'expéditeur (via une connexion chiffrée). La plateforme envoie alors une notification au destinataire, qui pourra ensuite récupérer le message et son contenu dans l'environnement sécurisé.

### BONNES PRATIQUES

- S'abonner à un service de communication sécurisé pour échanger des documents ou des messages.
- Ne pas utiliser de service gratuit sur internet dont les conditions d'utilisation prévoient que le prestataire de services a le droit d'accéder au contenu ou de l'utiliser à quelque fin que ce soit, ou dont les serveurs ne sont pas localisés au Canada ou dont le fournisseur est une société étrangère.
- Prévoir, dans la lettre mandat, les mesures de sécurité qui seront mises en place pour assurer la confidentialité des échanges, ce qui peut inclure le choix d'une plateforme pour l'échange de documents.

9

# COMMUNICATION DE DOCUMENTS

## › EXTRANET

Une organisation peut héberger elle-même la plateforme d'échange sécurisé de documents et partager l'accès à ses ressources informationnelles en mettant des applications à la disposition de ses clients, par exemple pour échanger des documents. Les risques liés à la confidentialité de la communication sont ainsi mieux gérés. Toutefois, cette ouverture du réseau interne à l'externe risque d'affecter la sécurité liée à la conservation des documents si les plateformes ne sont pas adéquatement configurées.

### BONNES PRATIQUES

> Mettre en place les mesures de sécurité appropriées, notamment la mise à jour des applications, l'authentification à deux facteurs, la ségrégation du réseau afin d'isoler divers éléments (les applications, les données du client et les données de l'organisation).

> Procéder à un test d'intrusion, qui consiste à analyser la sécurité d'une infrastructure technologique en simulant une attaque.

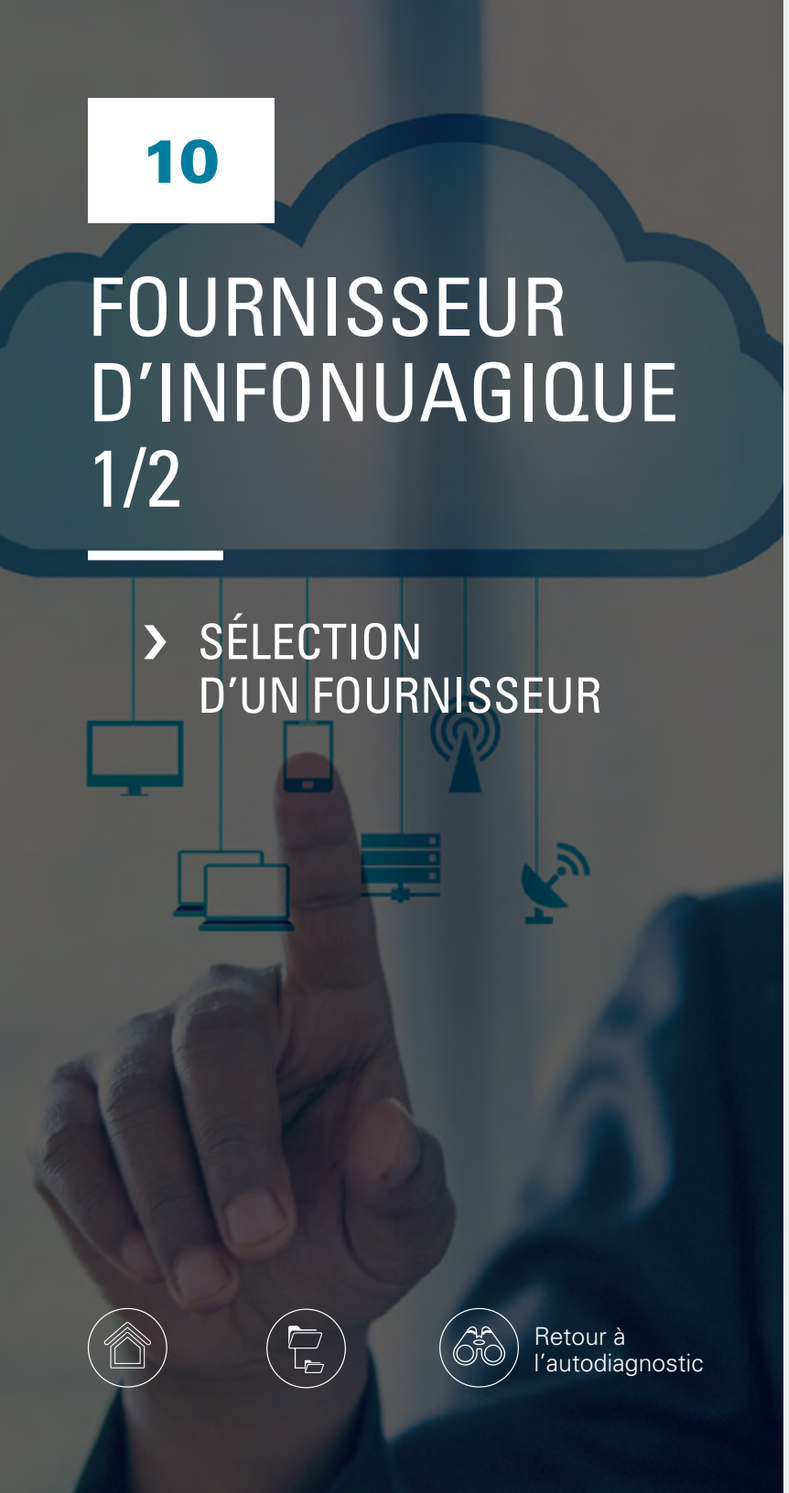
Retour à l'autodiagnostic

10

# FOURNISSEUR D'INFONUAGIQUE

| SÉLECTION D'UN FOURNISSEUR | ENTENTE AVEC LE FOURNISSEUR | LOCALISATION DES DONNÉES |
| --- | --- | --- |

Retour à l'autodiagnostic



10

# FOURNISSEUR D'INFONUAGIQUE 1/2

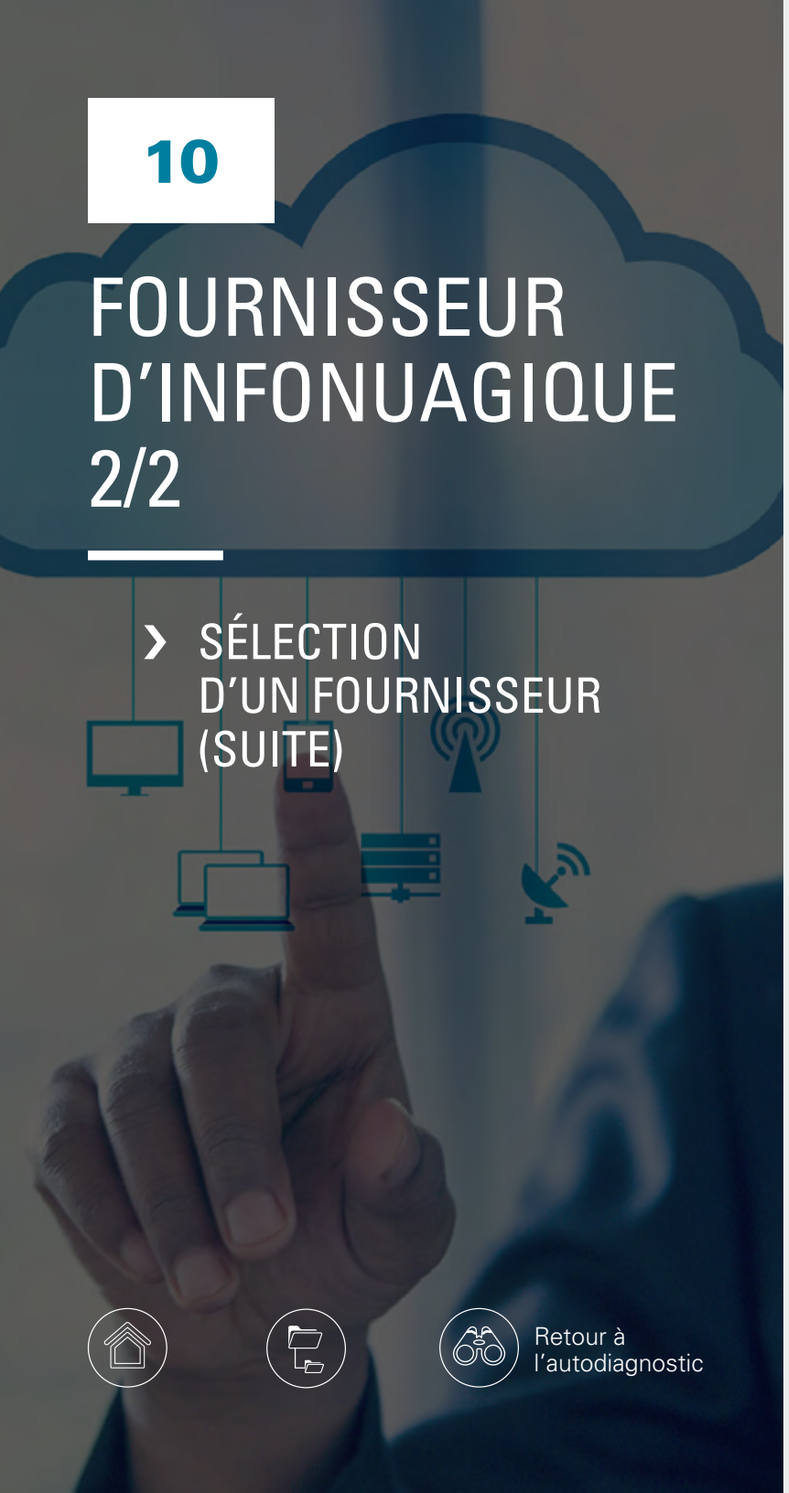
## › SÉLECTION D'UN FOURNISSEUR

L'implication d'un fournisseur externe est souvent nécessaire pour la planification ou l'exécution d'un projet en technologie de l'information. Si le fournisseur est aussi impliqué dans le développement de la solution (ex. : hébergement de données, création d'un logiciel ou analyse des données de l'entreprise), la proposition doit être analysée du point de vue de la sécurité de l'information.

### BONNES PRATIQUES

> Analyser les besoins quant à la sécurité et la confidentialité de l'information. Notamment, vérifier si le fournisseur :
  - émet et respecte des politiques écrites de confidentialité et de sécurité de l'information et si ces politiques sont en concordance avec vos propres politiques;
  - a mis en place des contrôles appropriés pour assurer la disponibilité, la sécurité et l'intégrité des données;
  - tient un registre des incidents ou des risques liés à la sécurité des données et s'engage à informer rapidement ses clients en cas d'incident pouvant les affecter.
> Vérifier la localisation des serveurs traitant ou hébergeant les données.
  - Où se situent physiquement ces serveurs?
  - Qui est responsable du lieu d'hébergement?
  - Le fournisseur a-t-il ses propres serveurs ou en sous-traite-t-il l'hébergement à une tierce partie connue et réputée, telle que Microsoft, Amazon, Google ou autre?
  - Le cas échéant, la tierce partie détient-elle des certifications ou effectue-t-elle des audits de sécurité (ex : ISO, SOC)?
  - Le fournisseur peut-il décider unilatéralement de transférer vos données dans une autre juridiction sans votre consentement?
  - Les données critiques sont-elles conservées au Québec?
  - Les copies de sauvegarde des données contenues sur les serveurs sont-elles hébergées au Québec?
> Évaluer les risques que présente une solution multi-locataires
  - La solution est-elle partagée avec d'autres clients?
  - Le cas échéant, quelles sont les mesures prises pour cloisonner les bases de données et s'assurer que seules les personnes autorisées pourront y accéder?
  - Quelles sont les possibilités de modifier la solution pour convenir à vos propres besoins et qui doit assumer les frais de ces modifications?
> Comprendre la propriété des données
  - À qui appartiennent les données échangées?
  - Qu'en est-il des données générées par le projet?
  - Les données vont-elles servir au fournisseur? Si oui, à quelles fins? Serviront-elles à entraîner un algorithme?
  - Le fournisseur peut-il accéder aux données? Si oui, peut-il les modifier, les utiliser pour ses activités, les vendre ou les partager avec des tiers?

Retour à l'autodiagnostic



10

# FOURNISSEUR D'INFONUAGIQUE 2/2

## › SÉLECTION D'UN FOURNISSEUR (SUITE)

Retour à l'autodiagnostic

## BONNES PRATIQUES (SUITE)

> Analyser les paramètres de conservation des données
  - Qui a la responsabilité de la destruction des données? Assurez-vous que votre accord soit requis avant la destruction de vos données ou qu'un délai de conservation soit précisé au contrat.
  - Des preuves de destruction sont-elles exigées par le contrat?
  - Le fournisseur a-t-il le droit de conserver des données et, si oui, sous quelles conditions?

> Prendre connaissance des procédures en cas de panne
  - Quelles sont les procédures en place chez le fournisseur potentiel pour répondre à des bris, des pannes ou toute autre situation pouvant occasionner des bris de service?
  - Quels sont délais pour répondre à un incident critique qui bloque les activités de votre entreprise ou qui met en péril la sécurité de l'information et le résoudre? Qu'en est-il pour un incident important qui bloque certaines fonctionnalités? Et pour un incident mineur qui n'affecte que quelques utilisateurs ou pour lequel des moyens de contournement sont possibles?

> Vérifier l'historique et la réputation des solutions proposées
  - Les solutions proposées par le fournisseur sont-elles réputées? Qu'en est-il du développeur?
  - D'autres organisations utilisent-elles ces solutions et, le cas échéant, des références sont-elles disponibles?
  - Un produit ou un service similaire est-il offert par un autre fournisseur? Si oui, posez-vous les questions précédentes au sujet de cette autre solution afin de faire un choix éclairé.

> S'assurer que la solution respecte les obligations liées à la protection des renseignements personnels
  - Des exigences spécifiques s'appliquent au Québec lorsque les données incluent des renseignements personnels. Par exemple :
    - Les données doivent être utilisées aux fins pour lesquelles un consentement est obtenu.
      - Les données seront-elles utilisées à d'autres fins par le fournisseur?
      - Des modalités contractuelles sont-elles en place pour vous permettre de respecter cette obligation?
    - Dans quelle juridiction les données seront-elles hébergées? À qui appartiennent les données? Une évaluation des facteurs relatifs à la vie privée devra être faite.
    - S'il s'agit d'un nouveau projet, d'un nouveau logiciel à implanter ou d'une modification à des solutions existantes, une évaluation des facteurs relatifs à la vie privée devra aussi être faite.

10

# FOURNISSEUR D'INFONUAGIQUE

## › ENTENTE AVEC LE FOURNISSEUR

Retour à l'autodiagnostic

Le terme infonuagique regroupe tout ce qui touche l'informatique délocalisée, c'est-à-dire des ressources informatiques (hébergement de données, logiciels, plateformes) qui sont, à divers degrés, sous la gestion d'un tiers. L'infonuagique comporte des avantages indéniables en termes de coûts et potentiellement en termes de sécurité de l'information, selon la maturité du partenaire retenu. Il demeure que la sécurité de l'information et le secret professionnel doivent faire l'objet de dispositions spécifiques dans l'entente de services.

### BONNES PRATIQUES

> Consulter un spécialiste en infonuagique pour mieux comprendre l'entente proposée et s'assurer que les exigences en termes de sécurité y sont clairement énoncées.

> Prévoir au contrat les modalités encadrant la gestion et la fin de l'entente avec le fournisseur d'infonuagique en ce qui concerne :

- la propriété des données;
- l'accès, la vente ou l'utilisation des données par le fournisseur;
- la localisation des serveurs traitant ou hébergeant les données;
- les préavis;
- la récupération des données et leur format;
- l'avis obligatoire en cas de bris de confidentialité, de vol des données ou de toute autre faille de sécurité;
- la possibilité d'un audit;
- l'utilisation de services de tierces parties;
- l'accès aux données et leur migration en cas de destruction des données, de cessation des services ou de la décision du fournisseur.

> Considérer la possibilité de souscrire une assurance couvrant la perte des données.

> Informer les clients, fournisseurs et autres partenaires que des données sont conservées sur un serveur externe.

10

# FOURNISSEUR D'INFONUAGIQUE

## › LOCALISATION DES DONNÉES

Lorsque les données se trouvent sur le réseau d'un fournisseur externe, le propriétaire des données peut perdre le contrôle de leur localisation. Les données peuvent aussi changer de localisation rapidement selon la disponibilité des ressources du fournisseur, qui peut lui-même faire affaire avec d'autres fournisseurs. S'il s'agit d'un fournisseur étranger, ou si les serveurs sont situés à l'extérieur du Québec ou du Canada, les données peuvent être assujetties à des lois étrangères.

Il existe des nuages géolocalisés dans lesquels les données circulent à l'intérieur de frontières établies, par exemple un nuage canadien, réduisant ainsi le risque de perte de contrôle sur la localisation des données.

### BONNES PRATIQUES

> Éviter les services d'infonuagique gratuits.

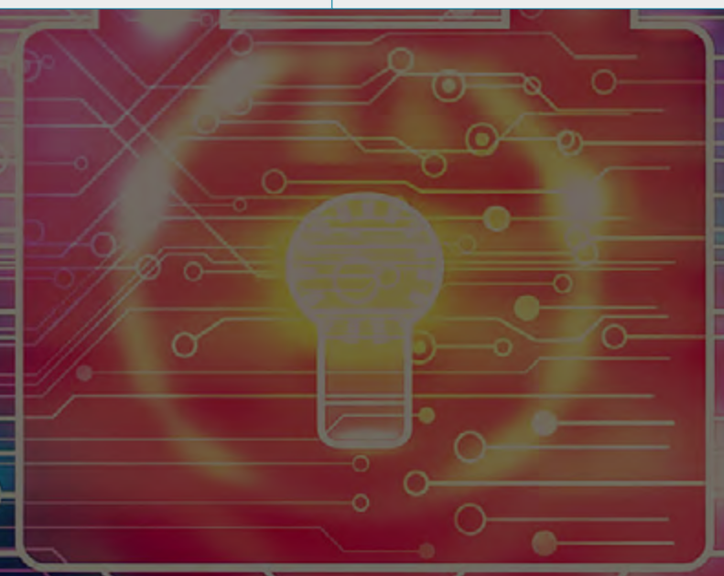
> Recourir à des fournisseurs québécois ou canadiens, surtout pour les actifs informationnels critiques ou confidentiels.

Retour à l'autodiagnostic

11

# SÉCURITÉ LIÉE AUX OPÉRATIONS

| | | |
|---|---|---|
| SAUVEGARDE DES DONNÉES | LOCALISATION DES COPIES DE SAUVEGARDE EN INFONUAGIQUE | SAUVEGARDE DES LOGICIELS ET MAINTIEN DES LICENCES |



Retour à l'autodiagnostic

11

# SÉCURITÉ LIÉE AUX OPÉRATIONS

## › SAUVEGARDE DES DONNÉES

Retour à l'autodiagnostic

La copie de sauvegarde assure la disponibilité des données en cas de sinistre. Elle pallie le risque de corruption des données (virus, tempête électromagnétique, bogue informatique, etc.) ou la perte de l'ensemble des données principales (vol, rançongiciel, etc.). La création des copies de sauvegarde et d'archivage nécessite deux processus différents.

Les logiciels disponibles offrent divers modes de sauvegarde. La méthode la plus courante consiste à procéder à intervalle plus ou moins long à une copie complète, puis par la suite à des copies qui n'incluront que les informations ayant été modifiées ou ajoutées depuis la dernière sauvegarde complète, requérant ainsi moins de temps et d'espace.

Les copies de sauvegarde doivent également être chiffrées. La copie de sauvegarde constitue le moyen de dernier recours pour récupérer des données. Elle doit donc être accessible et d'une grande fiabilité. La sécurisation de la clé de déchiffrement est primordiale.

### BONNES PRATIQUES

> Utiliser des logiciels éprouvés ou des routines automatisées.

> Procéder à une sauvegarde complète puis à des sauvegardes partielles selon un calendrier préétabli en fonction de la taille des systèmes à sauvegarder et du volume de nouvelles informations.

> Procéder à une sauvegarde complète avant de changer de fournisseur ou de mettre fin à une licence.

> Conserver les copies antérieures jusqu'à leur remplacement par une nouvelle copie complète.

> Lorsque la copie de sauvegarde est faite sur support physique, on doit :

- chiffrer le contenu du support;
- placer la clé de déchiffrement dans un endroit sécuritaire, tel un coffret de sûreté;
- conserver les mots de passe permettant de chiffrer et déchiffrer dans un gestionnaire de mots de passe.

> Si la sauvegarde est faite vers le serveur d'un prestataire de services, la connexion devrait être sécurisée et les données, chiffrées. Le chiffrement n'est pas essentiel si les mesures de sécurité du prestataire assurent une protection suffisante (au moyen d'un rapport d'expert par exemple).

> Prévoir dans le contrat avec le fournisseur d'infonuagique la façon dont seront récupérées les données en cas de nécessité ou pour effectuer des tests.

> Procéder périodiquement à des tests de récupération des données sur les copies les plus récentes.

> S'assurer que les copies de sauvegarde seront récupérables dans un format lisible et que l'organisation aura les systèmes nécessaires pour les utiliser le moment venu.

11

# SÉCURITÉ LIÉE AUX OPÉRATIONS

## › LOCALISATION DES COPIES DE SAUVEGARDE EN INFONUAGIQUE

Retour à l'autodiagnostic

Puisque la copie de sauvegarde doit pouvoir remédier à la perte de l'ensemble des données principales, elle doit en être séparée physiquement. La matérialisation d'un risque touchant l'ensemble des données principales ne doit pas affecter la copie de sauvegarde. La copie de sauvegarde doit donc être conservée dans un lieu distinct – un coffre-fort dans un autre édifice, par exemple.

De la même manière, la copie de sauvegarde doit être séparée logiquement pour éviter la corruption des données principales par un maliciel (tel un rançongiciel). Le support ne doit donc pas être connecté au système informatique une fois la copie prise. Le support utilisé doit être fiable et résister aux facteurs environnementaux (chaleur, humidité, chocs, frottements, électricité statique, etc.). Le volume d'information à sauvegarder déterminera le choix du support. Par exemple, disque dur externe pour les sauvegardes complètes et disques optiques pour les sauvegardes partielles.

Lorsque la sauvegarde est faite sur un serveur distant, chez un prestataire de services, les mesures à prendre sont les mêmes que pour l'utilisation de tout service infonuagique.

### BONNES PRATIQUES

- Conserver les copies de sauvegarde dans des lieux sécuritaires et distincts du lieu d'hébergement de l'ensemble des données principales.
- Ne pas laisser les disques durs externes branchés plus longtemps que nécessaire pour la prise de la sauvegarde.
- Considérer la sauvegarde comme n'importe quel autre service infonuagique et procéder aux mêmes vérifications, en plus de valider le mode de récupération des données.
- Éviter les services infonuagiques gratuits, les nuages délocalisés ou encore localisés ailleurs qu'au Canada et les fournisseurs étrangers.
- Choisir des supports d'information fiables en fonction de leur résistance aux facteurs environnementaux défavorables et du volume d'information à héberger.
- Éviter l'utilisation de clés de mémoire pour sauvegarder des données qui peuvent être facilement perdues.

11

# SÉCURITÉ LIÉE AUX OPÉRATIONS

## › SAUVEGARDE DES LOGICIELS ET MAINTIEN DES LICENCES

Retour à l'autodiagnostic

Le maintien des capacités logicielles passe par la prise d'une copie de sauvegarde des logiciels et des configurations particulières des logiciels plus complexes.

Par ailleurs, le droit d'utiliser ces outils logiciels en vertu d'accords de licence doit être maintenu dans le temps.

### BONNES PRATIQUES

- Prendre une copie de sauvegarde des logiciels installés dans le système informatique (support physique ou fichier installateur téléchargé).
- Procéder à un inventaire et établir un processus de gestion des licences qui servira aussi à identifier les cas où le nombre de licences serait insuffisant pour l'usage fait des logiciels (trop d'utilisateurs, trop d'utilisateurs en parallèle, installation sur trop d'appareils).
- Maintenir en vigueur les licences des logiciels utilisés, plus particulièrement celles des logiciels spécialisés, afin de préserver l'accès aux données.
- Considérer la migration des fichiers vers un format plus pérenne aux fins de la conservation du dossier client.

12

# CONTINUITÉ DES AFFAIRES

## › GÉNÉRALITÉS

La résilience de toute organisation implique qu'elle puisse poursuivre ses activités malgré toutes sortes de perturbations. C'est notamment le cas des cabinets de professionnels, tels les CPA, qui ont souvent des délais à respecter et qui doivent conserver trace de leurs activités pendant une période donnée après la fin de leur mandat.

Afin que le CPA puisse poursuivre ses activités et satisfaire à ses obligations déontologiques, plusieurs mesures doivent être mises en place, dont un plan de continuité des affaires et un guide d'exécution de la marche à suivre en cas de perturbation majeure pouvant affecter une organisation (catastrophe, accident, épidémie, cyberattaque, rupture de la chaîne d'approvisionnement, fermeture subite d'un fournisseur d'infonuagique, etc.).

Il va sans dire que les perturbations qui peuvent affecter les ressources informationnelles doivent trouver écho dans pareil plan de continuité des affaires. Un manque de préparation pour faire face à ces perturbations pourrait ralentir la reprise des activités normales et dès lors, constituer un manquement déontologique dans la mesure où des services pourraient ne pas être rendus à temps. Or, l'exonération en cas de force majeure (si tant est qu'elle pourrait jouer) n'a effet que pendant la durée de l'empêchement.

### BONNE PRATIQUE

> Élaborer un plan de continuité des affaires qui inclut :
  - un volet prévention avec un plan de sauvegarde;
  - le plan à exécuter en parallèle en cas de sinistre, comprenant le déploiement de personnel, la reprise après sinistre et le retour à la normale ;
  - le plan de gestion de l'incident ayant causé l'arrêt des opérations;
  - le plan de communication;
  - un plan de test récurrent afin d'en valider le fonctionnement.

Retour à l'autodiagnostic

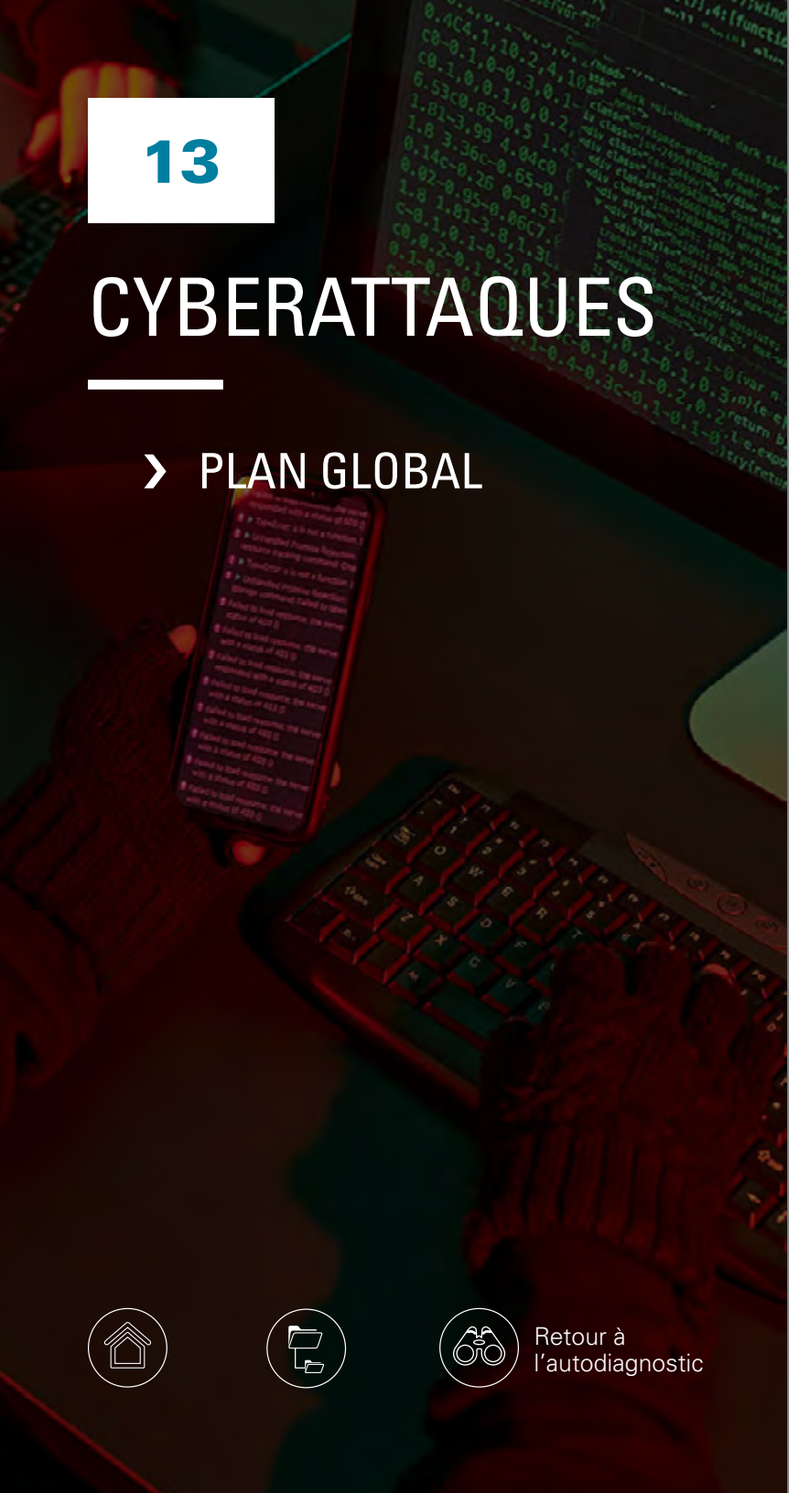
13

# CYBERATTAQUES

PLAN GLOBAL

QUE FAIRE EN CAS DE CYBERATTAQUE

Retour à l'autodiagnostic



13

# CYBERATTAQUES

## › PLAN GLOBAL

Retour à l'autodiagnostic

Il ne s'agit pas de directives exhaustives à suivre, mais plutôt de pistes pour structurer la gestion d'une cyberattaque.

## Mettre le plan d'intervention en œuvre (si vous en avez un)

### 1- Impliquer des experts

> Contacter votre équipe TI. Au besoin, recourir à des spécialistes externes en cybersécurité, notamment un conseiller juridique.

> Mesurer l'ampleur du problème :

- De quel type d'attaque s'agit-il ?
- Quand la brèche s'est-elle produite ou depuis quand est-elle ouverte?
- Quels sont les fichiers et les systèmes touchés?
- Quelles sont les parties prenantes touchées par cette attaque? Dresser une liste exhaustive comprenant, par exemple, les équipes internes précises et les partenaires externes, selon le cas.
- Quelles sont les incidences potentielles, notamment sur vos systèmes, vos clients, vos fournisseurs, votre réputation et vos finances?
- Quelles sont les procédures à suivre et les règlements et les obligations auxquels votre organisation est soumise (par exemple les lois qui concernent la protection des données et les clauses de vos ententes contractuelles)?

> Avertir votre assureur.

### 2- Corriger les problèmes et colmater la faille

> Prévoir les actions à entreprendre à court terme (heures), moyen terme (jours) et long terme (années) pour gérer la cyberattaque elle-même.

> Structurer et mettre en œuvre un plan de reprise des activités, dans la mesure du possible.

### 3- Planifier le retour à la normale

> Une fois que l'attaque est gérée, déterminer la marche à suivre pour assurer la reprise des activités normales.

> Réaliser une analyse rétrospective de l'incident pour en documenter la cause et les répercussions, ainsi que les leçons qu'on en tire. Il faut aussi dans bien des cas sauvegarder les preuves de l'incident, qui peuvent être requises en cas de poursuite.

13

# CYBERATTAQUES

## › QUE FAIRE EN CAS DE CYBERATTAQUE

Retour à l'autodiagnostic

Idéalement, un plan spécifique contre les cyberattaques devrait être préparé en amont, alors que les dirigeants ont le temps et les informations nécessaires à la prise de décision. L'objectif premier est de pouvoir réagir plus rapidement au moment de l'incident. Même s'il est impossible de se prémunir contre toutes les attaques, une bonne préparation passe par la rédaction de plans de réponse adaptés pour documenter les étapes à suivre selon le type d'attaque.

Le plan global ne devrait pas être trop détaillé afin d'être modulable en fonction des circonstances et de la taille de l'organisation. Il devrait notamment préciser :

> les indicateurs à surveiller pour déclencher le plan de crise;
> la chaîne de commandement;
> le rôle de chaque intervenant dans la crise;
> l'emplacement où se trouvent les informations nécessaires pour régler les problèmes les plus critiques pour l'organisation.

### Structure et personnes impliquées

Même si la cyberattaque peut paralyser toute l'organisation, c'est le plus souvent une seule équipe qui est en mesure de régler le problème. Les efforts du reste de l'organisation seront tournés vers la continuité des affaires et la reprise des activités normales.

Un responsable est désigné pour mettre en œuvre le plan de crise, dans la bonne séquence selon la situation. Il rend compte de l'évolution de la situation à un comité d'urgence, dont la composition et la fréquence des rencontres peut varier en fonction de l'événement. Par ailleurs, il peut être fort utile de retenir les services d'un conseiller juridique dès le début de la crise.

> Attention : les compétences techniques pointues ne sont pas absolument nécessaires en gestion de crise. Ce sont les compétences humaines qui priment pour prendre des décisions rapides et avec un certain détachement. La réaction au sentiment d'urgence doit être mise en équilibre avec la nécessité de rassurer les parties prenantes.
> Le responsable de l'exécution du plan de crise n'est pas nécessairement le chef des technologies.

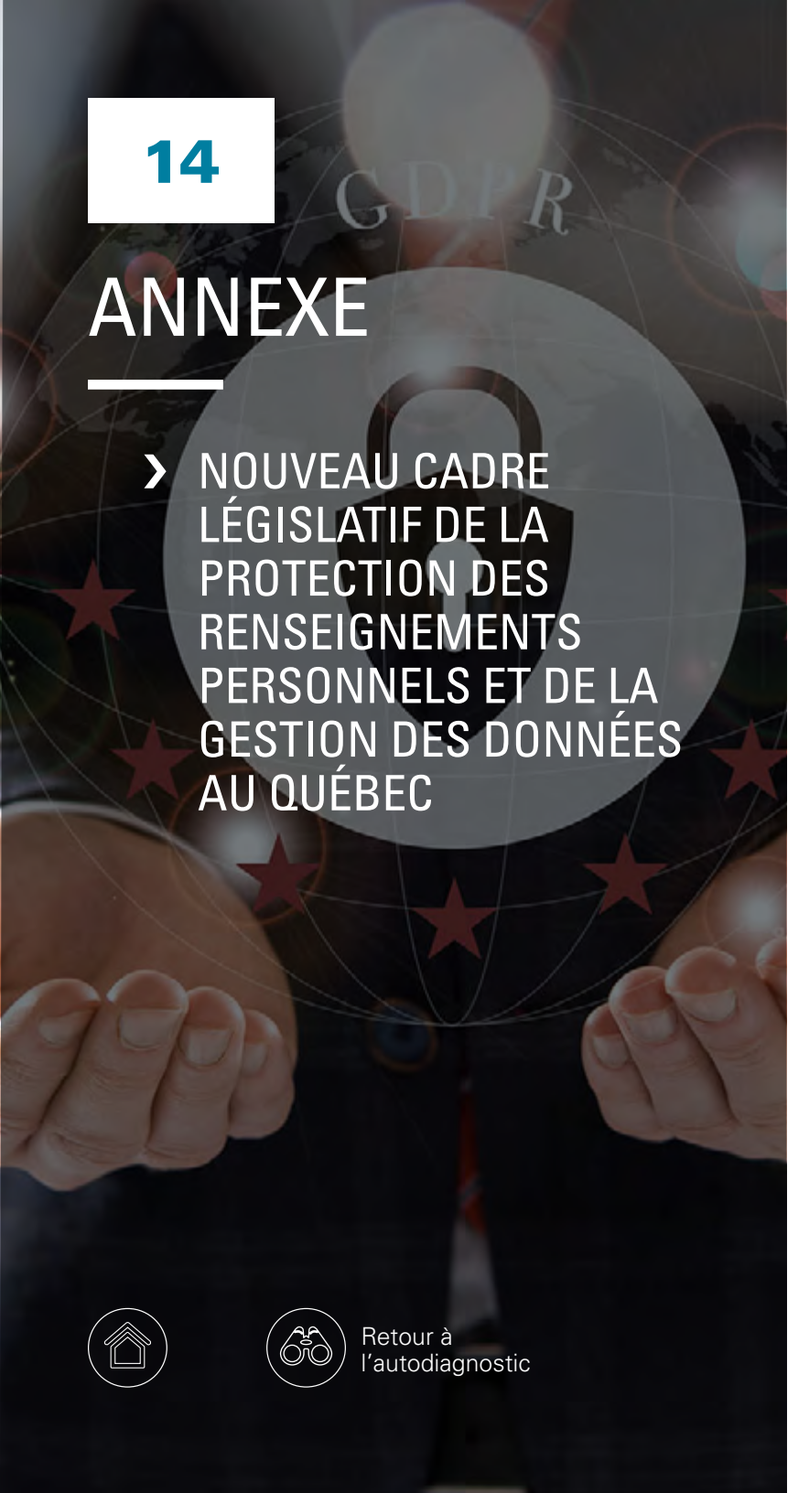
Le conseil d'administration doit être tenu informé mais pas impliqué directement dans la gestion de la crise. La perspective à plus long terme du conseil est essentielle pour une éventuelle reprise des activités.

### Communications

La communication est un élément clé de la gestion de crise. Les parties intéressées sont nombreuses et variées et les messages à transmettre diffèrent selon le public cible. Il est primordial de déterminer à qui revient la responsabilité de rédiger et d'approuver les communications.

### Parties prenantes

> Déterminer vos obligations juridiques et contractuelles, notamment auprès d'entités comme l'AMF, la Commission d'accès à l'information, certains créanciers, fournisseurs, assureurs ou clients.
> Identifier les autres parties prenantes, comme les équipes touchées, les équipes qui ne sont pas touchées et les autres collaborateurs.
> Obtenir un avis juridique, notamment sur les informations à partager et les avis à donner.
> Déterminer qui a l'autorité de communiquer avec quelle instance et qui doit avoir en main les informations à jour.



14

# ANNEXE

## › NOUVEAU CADRE LÉGISLATIF DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE LA GESTION DES DONNÉES AU QUÉBEC

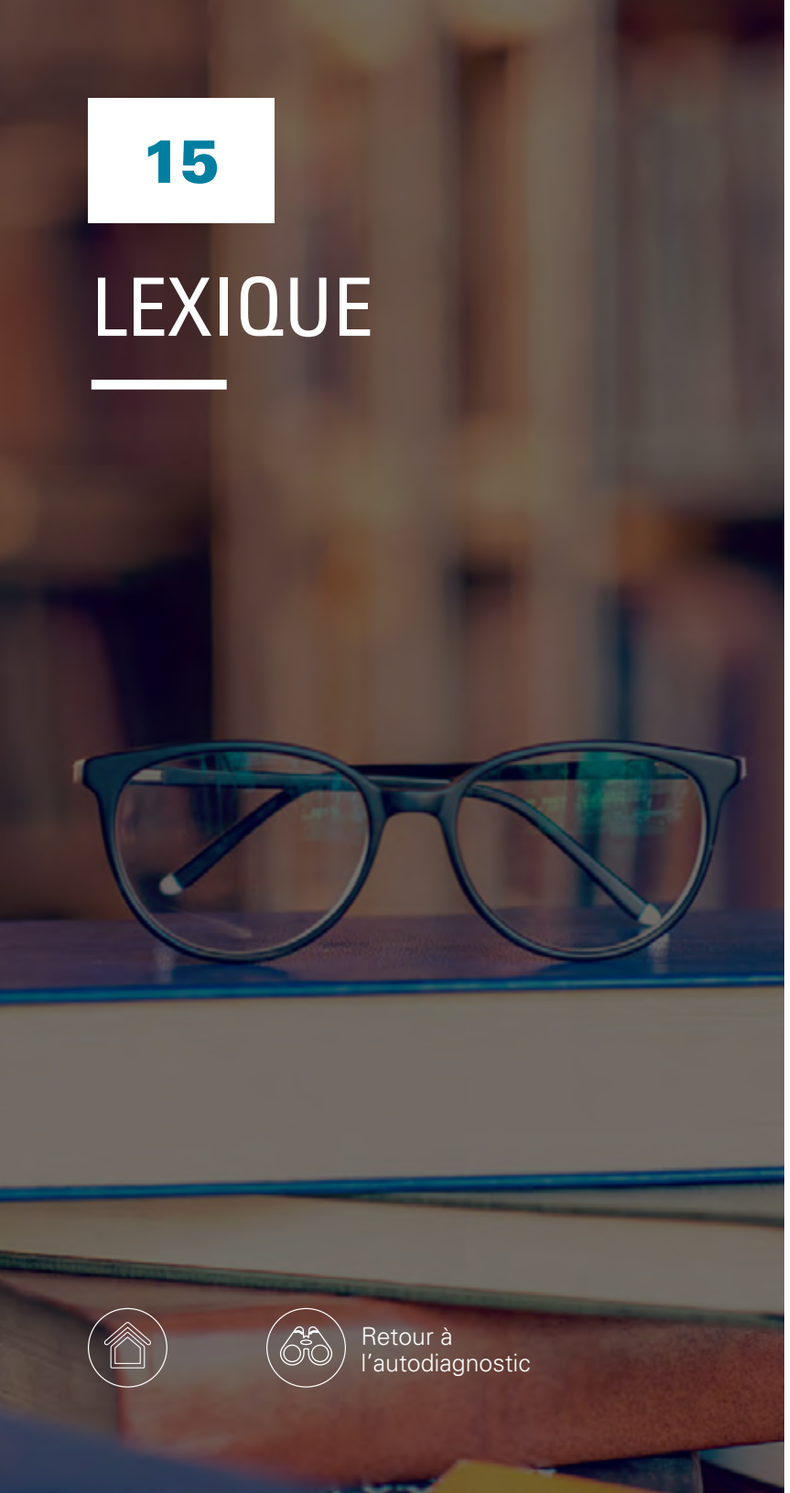
Retour à l'autodiagnostic

### Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25)* a été adoptée et sanctionnée en septembre 2021. L'entrée en vigueur des dispositions de la Loi s'étale jusqu'en 2024.

La *Loi 25* modifie substantiellement la *Loi sur la protection des renseignements personnels dans le secteur privé* (secteur privé) et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (secteur public). Elle impose de nouvelles obligations aux entreprises qui font affaire au Québec en matière de gouvernance des données personnelles. Elle modifie également le cadre applicable à la cueillette, la conservation, l'utilisation, la communication et la destruction des données.

La Commission d'accès à l'information met à votre disposition un site évolutif qui présente l'incidence de cette modernisation tant sur les citoyens que sur les entreprises et les ministères et organismes, ainsi qu'une ligne de temps qui permet de visualiser le calendrier d'entrée en vigueur des changements à venir.



15

# LEXIQUE

Retour à l'autodiagnostic

| Expression | Définition |
|---|---|
| Actif informationnel | Consiste en l'information elle-même, peu importe son support (papier ou technologique), ainsi que les systèmes utilisés pour son traitement, son utilisation, sa conservation et sa communication interne et externe. |
| Accès logique | Accès à un système d'information contrôlé par un protocole d'identification, d'authentification et d'autorisation. |
| Accès physique | Accès à un emplacement, un immeuble, un local, des infrastructures matérielles informatiques (salles des serveurs) ainsi qu'à de l'équipement spécifique (comme un coffret de sûreté). |
| Actif informationnel | Consiste en l'information elle-même, peu importe son support (papier ou technologique), ainsi que les systèmes utilisés pour son traitement, son utilisation, sa conservation et sa communication interne et externe. |
| AVEC | Acronyme signifiant *apportez votre équipement personnel de communication* et désignant le mode de travail selon lequel un employeur permet à son employé ou exige de lui qu'il utilise son matériel électronique personnel dans le cadre de son travail. |
| Clé de chiffrement | Clé qui convertit des données pour en rendre la compréhension impossible à toute personne qui n'a pas la clé de déchiffrement. |
| Clé de mémoire | Petit support amovible ou minidisque dur prenant la forme d'une clé ou d'un porte-clés, qui permet de stocker et de transporter des données dans le but de les transférer d'un ordinateur à un autre en s'insérant dans les ports USB. |
| Entente sur les niveaux de service | Entente écrite entre un fournisseur et un client où sont précisés les niveaux de service pour chaque service assuré par le prestataire.<br>Les niveaux de service couvrent notamment les heures de service, la disponibilité du service, le soutien à la clientèle, les niveaux de production, l'information sur la sécurité attendue, les frais et la terminologie. |
| Géoblocage, géodéblocage | Action de limiter l'accès à des ressources en ligne en fonction de la situation géographique de l'utilisateur. |
| Identifiant | Ensemble formé du nom d'un utilisateur et de son mot de passe, servant à valider son identité auprès d'un système. |
| Piratage psychologique | Tromperie qui résulte d'échanges entre individus afin d'extorquer des informations dans le but de pénétrer frauduleusement dans un système ou d'autrement frauder une organisation. |
| Réseau privé virtuel | Réseau établi en créant des liaisons permanentes spécialisées entre réseaux internes à travers des réseaux publics afin de répondre aux besoins en partage des ressources des utilisateurs. |
| Valeur de hachage | Valeur résultant du hachage – l'opération qui consiste à appliquer une fonction mathématique permettant de créer l'empreinte numérique d'un message, en transformant un message de taille variable en un code de taille fixe, en vue de son authentification ou de son stockage. |