POL 49-02
Glossaire – Sécurité de l'information
Direction Technologies de l'information

En vigueur : 2022-06-30	Approbation : Président-directeur-général Conseil d'administration
Révisé le : 2022-10-13	

Palais
des congrès
de Montréal

TERME OU ACRONYME	DÉFINITION
Accès à distance	Tout accès distants à des actifs informationnels de L'organisation réalisés en dehors de ses locaux à l'exclusion des activités de télétravail. Ce type d'activité est souvent réalisé par des fournisseurs de services qui gèrent des équipements à distance.
Accès public	Accès à Internet à travers un réseau partagé situé dans un lieu public tel un café Internet, un hôtel ou un aéroport.
Accès sécurisé	Accès à un réseau informatique, tel Internet, selon une méthode permettant de contrôler l'autorisation d'accès d'un utilisateur (code d'identification, mot de passe, etc.).
Acte malveillant	Action qui consiste en un acte (ou une tentative d'acte), isolé ou répété, commis dans l'intention de nuire à l'entreprise, ses membres, dirigeants, clients ou usagers.
Actif informationnel	Toute information que possède L'organisation (à titre de propriétaire ou de simple possesseur), peu importe son support (papier, électronique ou autre), ainsi que les systèmes utilisés pour son traitement, utilisation, stockage, conservation et communication.
Administrateur (d'un mécanisme de contrôle d'accès)	Un administrateur d'un mécanisme de contrôle d'accès est un membre du personnel qui a été désigné pour administrer et contrôler les demandes d'accès à un environnement informatique ou à l'une de ses ressources.
Algorithme	Ensemble de règles opératoires dont l'application permet de résoudre un problème énoncé au moyen d'un nombre fini d'opérations. Un algorithme peut être traduit, grâce à un langage de programmation, en un programme exécutable par un ordinateur.
Altération	Toute modification qui a pour effet de changer les caractéristiques, l'état normal ou la nature d'un actif informationnel.
Analyse du risque (sécurité de l'information)	Évaluation du risque en fonction des sources de risque, de leur plausibilité d'occurrence et de leurs impacts.
Appareil personnel (voir Système d'information personnel)	Tout système d'information fourni par l'utilisateur, par opposition aux systèmes d'information fourni par l'employeur.
Application (informatique)	Logiciel, progiciel, programme ou ensemble de programmes informatiques permettant d'effectuer un traitement particulier sur un système d'information.

Authentifiant (voir compte d'accès)	Informations fournies lors d'un processus d'authentification afin de prouver son identité pour obtenir l'accès à un actif informationnel. Le couple code usager (identifiant) et mot de passe (preuve d'identité) est un authentifiant fréquemment utilisé.
Authentification	L'authentification est une phase qui permet à l'utilisateur d'apporter la preuve de son identité avant de lui permettre l'accès à des actifs informationnels. Elle intervient après la phase dite d'identification. Elle permet de répondre à la question: "*Êtes-vous réellement cette personne?*".
Authentification à double facteur (voir Authentification multi facteur, Authentification forte)	L'authentification à double facteur est un processus de sécurité par lequel l'utilisateur fournit deux modes d'authentification à partir de catégories de données distinctes : l'une se présente généralement sous la forme d'un jeton physique, comme une carte, et l'autre sous forme d'informations mémorisées, par exemple un code de sécurité.
Authentification forte (voir Authentification à double facteur, Authentification double)	L'authentification à double facteur est un processus de sécurité par lequel l'utilisateur fournit deux modes d'authentification à partir de catégories de données distinctes : l'une se présente généralement sous la forme d'un jeton physique, comme une carte, et l'autre sous forme d'informations mémorisées, par exemple un code de sécurité.
Authentification multi facteur (voir Authentification à double facteur, Authentification forte)	L'authentification à double facteur est un processus de sécurité par lequel l'utilisateur fournit deux modes d'authentification à partir de catégories de données distinctes : l'une se présente généralement sous la forme d'un jeton physique, comme une carte, et l'autre sous forme d'informations mémorisées, par exemple un code de sécurité.
Autorisation	Attribution d'un privilège d'accès à une entité par une autorité.
Autorité d'enregistrement (RA)	Dans le cadre de la délivrance de certificats cryptographique l'autorité d'enregistrement (« *Registration Authority* ») est l'entité qui vérifie que les détenteurs de certificat sont identifiés, que leur identité est authentique et que les contraintes liées à l'usage d'un certificat sont remplies, tout cela conformément à la politique de l'entreprise. L'autorité d'enregistrement peut avoir également pour tâche de traiter les demandes de révocation de certificats.).
Autorité de certification (CA)	En cryptographie, une Autorité de Certification (« *Certificate Authority* ») est un tiers de confiance permettant d'authentifier l'identité des correspondants. Une autorité de certification délivre des certificats décrivant des identités numériques et met à disposition les moyens de vérifier la validité des certificats qu'elle a fournis.
Brèche de sécurité (Voir Incident de cybersécurité)	Événement qui porte atteinte à l'authenticité, à la confidentialité, à la disponibilité ou à l'intégrité.

Bris de service	Interruption d'un service occasionnés par une défaillance technique ou un manquement à un processus d'affaires ayant un impact sur les fonctions d'affaires de l'organisation.
Cadre normatif de sécurité de l'information (*Encadrements*)	Ensemble de documents, constitués à la base par la politique de sécurité de l'information. Il comprend l'ensemble des directives utilisées pour préciser le cadre de cette politique.
Carte d'identité	Carte d'accès émise par L'organisation munie d'une photographie et utilisée comme preuve d'identité.
Catégorisation (Voir Classification)	Processus à travers lequel on attribue une cote de confidentialité, de disponibilité et d'intégrité à un groupe d'actifs informationnels similaires ou supportant un processus d'affaires. Cette cote permet d'établir la criticité du groupe d'actifs en lien avec sa fonction dans les processus d'affaires de l'organisation.
Certificat	Document électronique qui permet d'attester de l'identité de son détenteur.
Chiffrement	Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.
Classification (Voir Catégorisation)	Processus à travers lequel on attribue une cote de confidentialité, de disponibilité et d'intégrité à un actif informationnel. Cette cote permet d'établir la criticité de l'actif en lien avec sa fonction dans les processus d'affaires de l'organisation.
Clé asymétrique	Le chiffrement asymétrique est une méthode de chiffrement qui utilise deux clés : une tenue secrète et connue d'une seule personne (la clé privée) et une autre qui est publique et à la disposition de tous (la clé publique). Les deux clés ont une interrelation mathématique, mais il est impossible d'en dériver une de l'autre. Parmi les chiffrements asymétriques bien connus, on trouve l'algorithme de Diffie-Hellman, RSA et DSA.
Clé de chiffrement (voir clé cryptographique)	Une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature). Une clé de chiffrement peut être symétrique ou asymétrique : dans le premier cas, la même clé sert à chiffrer et à déchiffrer ; dans le second cas on utilise deux clés différentes, la clé de chiffrement est publique alors que celle servant au déchiffrement est gardée secrète (la clé secrète, ou clé privée, ne peut pas se déduire de la clé publique).

Clé de cryptographique (voir clé de chiffrement)	Une clé est un paramètre utilisé en entrée d'une opération cryptographique (chiffrement, déchiffrement, scellement, signature numérique, vérification de signature). Une clé cryptographique peut être symétrique ou asymétrique : dans le premier cas, la même clé sert à chiffrer et à déchiffrer ; dans le second cas on utilise deux clés différentes, la clé cryptographique est publique alors que celle servant au déchiffrement est gardée secrète (la clé secrète, ou clé privée, ne peut pas se déduire de la clé publique).
Clé privée	Une clé cryptographique peut être symétrique ou asymétrique : dans le premier cas, la même clé sert à chiffrer et à déchiffrer ; dans le second cas on utilise deux clés différentes, la clé cryptographique est publique alors que celle servant au déchiffrement est gardée secrète (la clé secrète, ou clé privée) et ne peut pas se déduire de la clé publique.
Clé publique	Une clé cryptographique peut être symétrique ou asymétrique : dans le premier cas, la même clé sert à chiffrer et à déchiffrer ; dans le second cas on utilise deux clés différentes, la clé cryptographique est publique alors que celle servant au déchiffrement est gardée secrète (la clé secrète, ou clé privée) et ne peut pas se déduire de la clé publique.
Clé symétrique	Le chiffrement symétrique est le chiffrement cryptographique le plus ancien et le plus utilisé. Dans ce procédé, la clé qui déchiffre le texte chiffré est la même que la clé qui chiffre le texte en clair. Elle est souvent appelée clé secrète.
Cloud (voir Infonuagique)	Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation. Voir également : SaaS, IaaS et PaaS
Code source	Le code source est un texte qui représente les instructions d'un programme telles qu'elles ont été écrites dans un langage de programmation sous une forme humainement lisible par un programmeur.
Collaborateur (Voir Partenaire)	Individu ou groupes d'individus qui participent aux activités de l'organisation sans détenir le statut d'employés, de consultants ou de fournisseurs. Dans certains cas, les activités d'un collaborateur peuvent requérir l'utilisation d'un actif informationnel propriété de l'organisation.
Composante	Équipement faisant parti d'un ensemble technologique qui supporte une fonction d'affaires.
Composantes importantes	Tout actif informationnel classifié comme élevé ou très élevé ou considéré comme tel par une procédure de sécurité.

Compte d'accès (voir Identifiant)	Code attribué à une personne ou à toute autre entité et lui permettant de s'identifier lors de l'accès à un actif informationnel protégé. Il n'est pas associé à une preuve d'identité.
Compte d'accès à privilèges élevés	Compte d'accès attribué à un utilisateur afin de lui permettre d'administrer les environnements, plateformes et systèmes ou de passer outre les mesures et contrôles mis en place pour des raisons de support.
Compte d'accès local	Compte d'accès qui n'est pas défini dans le répertoire central d'identités de l'organisation.
Compte d'accès partagé (générique)	Compte d'accès devant être partagé entre plusieurs individus, soit : • Pour des raisons techniques incontournables empêchant l'utilisation d'un compte d'accès individuel; • Pour en faciliter la gestion, s'il s'agit d'un compte d'accès à privilèges restreints et qu'aucune traçabilité des actions posées par son détenteur n'est requise.
Compte d'accès personnel	Compte d'accès attribué à l'usage exclusif d'un individu.
Compte de services	Compte d'accès attribué à un système ou une application habituellement utilisé dans des contextes non-interactifs s'exécutant sur un serveur ou des tâches planifiées exécutées automatiquement.
Confidentiel(le)	Caractéristique d'une information qui, par sa nature ou en raison des exigences de l'organisation, de la loi et des règlements, des contrats, des Directives ou des normes, n'est et ne doit être ni disponible au public, ni divulguée aux personnes, entités ou processus non autorisés.
Consultant	Désigne habituellement un non-salarié qui a accès à un actif informationnel de l'organisation et qui occupe une fonction normalement attribuée à un *Employé*. Il se distingue d'un fournisseur de service qui peut réaliser des activités à distance.
Contrôle d'accès	Mesure de protection permettant de contrôler l'accès à un environnement informatique, qui comprend l'identification de l'utilisateur effectuant l'accès, son authentification, l'autorisation d'accès aux ressources, la journalisation et le suivi des accès.
Cote DIC	Désigne le niveau de criticité d'un actif informationnel sous une forme numérique reprenant ceux de la classification de l'atif. Une cote DIC de 232 correspond à un actif classifié « 2 » en Disponibilité, « 3 » en Intégrité et « 2 » en Confidentialité.
Criticité	Détermination et hiérarchisation de l'impact que peut avoir un événement sur un système d'un point de vue financier, d'affaires ou fonctionnel.

Critique (voir information sensible)	Désigne tout actif informationnel qui n'est pas classifié publique ou interne ou donc la catégorisation est au-delà du seuil de tolérance défini par l'organisation.
Cryptographie	Ensemble des techniques recourant à des combinaisons d'algorithmes et de valeurs secrètes, appelées clés, utilisées à des fins de contrôle dans des procédures comme le chiffrement, l'authentification, la non-répudiation et la signature électronique.
Cybersécurité (Voir Sécurité de l'information)	Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. L'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées. A la différence du terme "Sécurité de l'information", celui-ci adresse uniquement les environnements numériques (ex.: serveurs, infonuagique, etc.)
Cycle de vie de l'information	La période de temps couvrant toutes les étapes d'existence de l'information dont celles de la définition, de la création, de l'enregistrement, du traitement, de la diffusion, de la conservation et de la destruction de cette information.
Dérogation	Processus généralement approuvé par le responsable de la sécurité de l'information qui permet d'outrepasser un requis de sécurité. Ce processus permet de documenter l'écart, le risque associé à celui-ci, les mesures compensatoires mises en place et l'approbation du risque résiduel.
Destruction sécuritaire	Processus à travers lequel un support contenant de l'information est détruit de telle sorte que les informations contenues ne peuvent plus jamais être récupérées
Directive	Découle d'une politique et en précise le cadre. Peut être un document corporatif ou départemental et précise les règles de conduite internes, les objectifs opérationnels à atteindre et départage les responsabilités entre les différentes unités d'affaires.
Disponibilité	Propriété d'un actif informationnel d'être accessible en temps voulu et de la manière requise par une personne ou une entité autorisée.
Donnée sensible (voir information sensible)	Une information qui, si elle est révélée au public, nuirait aux entités qu'elle concerne. Ce type d'information exclut habituellement les informations de nature publique et interne à une organisation.
Données auxiliaires	Les données auxiliaires sont des données générées lors de la prestation de services d'un le fournisseur : statistiques d'utilisation, regroupements thématiques, données de géolocalisation, données démographiques, etc. Elles se différencient des données initialement fournies par le client mais peuvent contenir celles-ci dans un format différent.
Données de production	Données d'affaires stockées, traitées et communiquées par l'un ou l'autre des systèmes d'information exploités par les technologies de l'information.

Données de test	Données utilisées en remplacement des données de production dans les systèmes d'information dans les environnements autres que ceux de production.
Employé	Désigne habituellement tout individu qui a accès à un actif informationnel de l'organisation quel que soit son statut d'emploi (stagiaire, étudiant ou salarié permanent/temporaire, consultant).
Encadrements (Voir Cadre normatif de sécurité de l'information)	Ensemble de documents, constitués à la base par la politique de sécurité de l'information. Il comprend l'ensemble des directives utilisées pour préciser le cadre de cette politique.
Énoncé de sécurité	Description complète des mesures de sécurité techniques et non techniques requises pour protéger adéquatement un actif informationnel.
Équipement mobile (Voir Informatique mobile)	Un équipement mobile désigne tout système d'information utilisé par un individu dans ses déplacements. Les ordinateurs portables, téléphones intelligents, tablettes, périphériques de stockage amovibles tels que clés USB sont des exemples d'informatique mobile.
Évaluation du risque	Processus de comparaison du risque estimé avec des critères de risque donnés pour en déterminer l'importance. Une évaluation du risque est habituellement basée sur une approche normalisée reconnue par l'industrie (ex. Méhari, Octave, ISO 31000, etc.).
Évaluation sommaire du risque	Processus accéléré qui permet aux organisations d'obtenir un score rapide du niveau de risque associé à un nouveau projet ou une acquisition. Le processus est qualifié de « sommaire » par l'utilisation de scénarios de risques prédéfinis par l'organisation et l'utilisation d'un questionnaire limitant la subjectivité de l'évaluateur.
Événement de sécurité	Un événement de sécurité est un événement pouvant indiquer que les systèmes ou les données d'une entreprise ont été compromis ou que les mesures mises en place pour les protéger ont échoué. En informatique, un événement est tout ce qui a une importance pour le matériel ou les logiciels du système et un incident est un événement qui perturbe les opérations normales. Les événements de sécurité se distinguent généralement des incidents de sécurité par leur degré de gravité et le risque potentiel associé pour l'organisation.
Exception	Non-conformité dont le risque résiduel est **faible** et accepté par le propriétaire de l'actif informationnel impacté ou situation de non-conformité **préexistante** pour laquelle aucun plan d'action n'est prévu pour des raisons d'affaires ou de limitations technologiques.

Exploitant	Responsable de l'exploitation de l'actif informationnel qu'il soit de nature technologique ou applicative. L'Exploitant coordonne et réalise les activités et les processus nécessaires pour fournir les services technologiques au propriétaire d'un actif informationnel à des niveaux de services convenus.
Fédération des identités	Concept qui vise à mettre en place une centralisation des données d'identité. Ainsi un utilisateur ne se connectera qu'une unique fois par session auprès d'une structure reconnue qui lui fournira la preuve de son identité (sous forme de jeton). L'utilisateur le présentera aux autres ressources qui souhaitent s'assurer de son identité, sans qu'il n'ait à dérouler une nouvelle procédure d'authentification.
Fournisseur	Un fournisseur est une personne physique ou morale qui fournit des biens ou des services à l'organisation. Ceci inclut, notamment les entrepreneurs et sous-entrepreneurs, les partenaires d'affaires, les prestataires de services et les représentants et utilisent habituellement leurs propres équipements informatiques. Les consultants qui comblent des fonctions normalement occupées par un *Employé* sont expressément exclus de cette définition.
Gabarit ou standard de configuration	Document technique qui détaille la configuration standard approuvée d'un système d'information. Ce document technique fournit également les contrôles de sécurité qui doivent être mis en place.
Gestion des changements	Processus responsable de contrôler le cycle de vie de tous les changements, facilitant la réalisation de changements bénéfiques avec un minimum d'interruption des services informatiques.
Grille d'impact	Cette grille est utilisée à la fois pour la gestion du risque ainsi que pour la classification des actifs. Elle permet de définir les différents niveaux d'impact et leurs critères en fonction des volets suivants : disponibilité, intégrité, confidentialité, clientèle, finances et réputation.
Guide de référence	Document fournissant des conseils et des recommandations aux gestionnaires ou aux spécialistes fonctionnels. Le *Guide de référence* vise à aider un intervenant à prendre des décisions dans un domaine spécifique afin d'améliorer la qualité d'une action. Un *Guide de référence* n'est pas obligatoire mais devrait être considéré dans la réalisation d'une activité spécifique.
Hachage (fonction de…)	On nomme fonction de hachage, de l'anglais « *hash function* », une fonction mathématique qui, à partir d'une donnée fournie en entrée, calcule une empreinte numérique servant à identifier rapidement la donnée initiale, au même titre qu'une signature pour identifier une personne. Les fonctions de hachage sont utilisées en cryptographie notamment pour reconnaître rapidement des fichiers ou des mots de passe.

IaaS	Une solution IaaS, ou *Infrastructure as a Service*, fournit l'infrastructure informatique, c'est-à-dire, la solution de virtualisation, les serveurs, les réseaux, et le stockage des données. Ce service infonuagique nécessite des compétences et de l'autonomie de la part de l'administrateur afin de gérer le système d'exploitation, les applications, les données, etc. L'IaaS permet ainsi de dématérialiser uniquement l'infrastructure matérielle.
Identifiant (Voir Compte d'accès)	Code attribué à une personne ou à toute autre entité et lui permettant de s'identifier lors de l'accès à un actif informationnel protégé. Il n'est pas associé à une preuve d'identité.
Identification	L'identification est une phase qui consiste à établir l'identité de l'utilisateur. Elle permet répondre à la question: "*Qui êtes-vous* ?". L'utilisateur utilise un identifiant (que l'on nomme "Compte d'accès", "Nom d'utilisateur") qui l'identifie et qui lui est attribué individuellement. Cet identifiant est unique.
Image	Version « virtuelle » d'un système d'information (système d'exploitation, applications, configuration) qui permet de reproduire une installation approuvée.
Impact significatif (ou critique)	Désigne un impact « Élevé » ou « Très Élevé » selon la grille d'impact de l'organisation.
Impartiteur	Entreprise spécialisée dans les prestations de services reliées à la prise en charge de la totalité ou d'une partie des ressources informatiques d'une entreprise ou d'une organisation.
Impartition (Services impartis)	Transfert de tout ou partie d'une fonction de l'organisation (administrative ou technologique) vers un partenaire externe.
Incident de sécurité	Un incident de sécurité est un événement indiquant qu'il pourrait y avoir, ou y avoir eu, une atteinte à la sécurité. Plus particulièrement, il s'agit d'un acte, d'un événement ou d'une omission pouvant entraîner la compromission de renseignements, de biens ou de services en rapport avec: (A) la sécurité des services, des systèmes de services ou de toute partie de ceux-ci; et (B) les exigences de la Politique de sécurité qu'elles soient ou non causées en totalité ou en partie par un acte ou une omission. Un incident de sécurité se distingue d'un incident opérationnel par sa sévérité en termes d'impacts, des cibles et de l'intention malicieuse présumée.
Incident opérationnel	Désigne un incident qui se produit ou est observé pendant la fourniture des services et qui a ou pourrait causer un impact négatif sur la fourniture ou la qualité des services qui n'est pas un incident de sécurité.

Indicateur de compromission	Un indicateur de compromission, en sécurité de l'information, est un artefact observé sur un réseau ou dans un système d'exploitation qui indique, avec un haut niveau de certitude, une intrusion informatique. Exemples d'indicateurs de compromission : signatures virales, adresses IP particulières, hash de fichiers malveillants, URLs ou noms de domaine de serveurs de commande et de contrôle de botnet. Une fois que les identificateurs ont été identifiés dans un processus de réponse aux incidents et de criminalistique informatique, ils peuvent être utilisés pour la détection précoce des tentatives d'attaque en utilisant des systèmes de détection d'intrusion et des logiciels antivirus.
Infonuagique (voir Cloud)	Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation. Voir également : SaaS, IaaS et PaaS
Information confidentielle (ou Renseignement confidentiel)	Tout renseignement utilisé pour la conduite des affaires de l'organisation qui n'est pas de nature publique. Les renseignements personnels sont tous des renseignements confidentiels.
Information sensible (voir donnée sensible)	Une information ou une connaissance qui, si elle est révélée au public, nuirait aux entités qu'elle concerne. Ce type d'information exclut habituellement les informations de nature publique et interne à une organisation.
Informatique mobile (Voir Équipement mobile)	L'informatique mobile désigne tout système d'information utilisé par un individu dans ses déplacements. Les ordinateurs portables, téléphones intelligents, tablettes, périphériques de stockage amovibles tels que clés USB sont des exemples d'informatique mobile.
Ingénierie sociale	Forme d'acquisition déloyale d'information et d'escroquerie, utilisée en informatique pour obtenir d'autrui, un bien, un service ou des informations clefs. Cette pratique exploite les failles humaines et sociales de la structure cible, à laquelle est lié le système informatique visé. Utilisant ses connaissances, son charisme, l'imposture ou le culot, l'attaquant abuse de la confiance, de l'ignorance ou de la crédulité des personnes possédant ce qu'il tente d'obtenir.
Intégrité	Propriété d'une information de n'être détruite ou altérée de quelque façon, sans autorisation.

Internet des Objets (IdO)	L'Internet des objets, ou IdO (en anglais « Internet of Things », ou IoT) caractérise des objets physiques connectés ayant leur propre identité numérique et capables de communiquer les uns avec les autres. D'un point de vue technique, l'IdO consiste en l'identification numérique directe et normalisée (adresse IP, protocoles smtp, http...) d'un objet physique grâce à un système de communication sans fil qui peut être une puce RFID, Bluetooth ou Wi-Fi.
Intranet	Sites web utilisés à l'interne de l'organisation pour la diffusion d'informations.
Journal	Relevé chronologique des opérations informatiques constituant un historique de l'utilisation des programmes et des systèmes sur une période donnée.
Journalisation	Enregistrement dans un journal informatique des événements informatiques et/ou de sécurité effectuées dans un système.
Logiciel	Programmes informatiques permettant d'effectuer un traitement particulier sur un ordinateur.
Logiciel malveillant (voir code malveillant, virus, *malware*)	Un virus ou logiciel malveillant (de l'anglais malware) est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté. De nos jours, le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les maliciels englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.
Matrice de risque	Matrice dont les axes adressent la potentialité et l'impact de la réalisation d'une menace sur un actif informationnel, définissant ainsi la gravité du risque généré par cette menace. Cette matrice identifie également le seuil de tolérance aux risques de l'organisation.
Mesure de sécurité (…de contrôle)	Dans le contexte d'une *Politique* ou d'une *Directive*, moyen concret qui assure, partiellement ou totalement, la protection de *l'Actif informationnel* contre une ou plusieurs menaces informatiques, et dont la mise en oeuvre vise à amoindrir la probabilité de survenance de ces menaces ou à minimiser les pertes qui en résultent.
Mise à niveau	Procédure consistant à modifier une application, un système, un logiciel ou une infrastructure pour en assurer l'évolution continue. Une mise à niveau peut être nécessaire suite aux recommandations d'un fournisseur, à l'évolution des technologies, à la découverte de nouvelles vulnérabilités, etc.
Mode d'opération (cryptographie)	En cryptographie, un mode d'opération est la manière de traiter les blocs de texte clairs et chiffrés au sein d'un algorithme de chiffrement par bloc.

Moindre privilège ou privilège d'accès minimal	Principe de sécurité de l'information consistant en l'octroi de privilèges d'accès restreints aux seuls actifs informationnels requis pour accomplir les tâches nécessaires à l'exercice des fonctions de la personne ou de toute autre entité.
Mot de passe	Authentifiant prenant la forme d'un code alphanumérique et attribué à un utilisateur, permettant à ce dernier d'obtenir l'accès à un ordinateur en ligne et d'y effectuer l'opération désirée.
Non-conformité	Non-conformité à un encadrement qui fait l'objet d'un plan d'action visant à mettre en place un correctif dans un délai défini, lorsque le risque résiduel est moyen, élevé ou très-élevé.
Non-répudiation	La non-répudiation signifie la possibilité de vérifier que l'envoyeur et le destinataire sont bien les parties qui disent avoir respectivement envoyé ou reçu le message. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.
PaaS	Une solution PaaS, ou *Platform as a Service*, fournit les services de l'IaaS (dématérialisation du matériel) ainsi que les applications middlewares : système d'exploitation, le serveur web, la base de données, etc. L'avantage de cette solution est son côté évolutif, ainsi qu'une pré-configuration de l'environnement technique.
Partenaire (Voir Collaborateur)	Individu ou groupes d'individus qui participent aux activités de l'organisation sans détenir le statut d'employés, de consultants ou de fournisseurs. Dans certains cas, les activités d'un partenaire peuvent requérir l'utilisation d'un actif informationnel propriété de l'organisation.
Parties prenantes	Une partie prenante est un acteur (individu, groupe ou organisation), concerné par une décision ou une action.
Phrase secrète	Le terme « phrase secrète » ou « phrase de passe » (en anglais, *passphrase*) désigne un mot de passe d'un nombre important de caractères. On parle de phrase de passe plutôt que de mot de passe parce que la phrase de passe contient souvent des suites de mots qui ressemblent parfois à une phrase pour des raisons mnémotechniques.
Plan anti-sinistre (voir Plan de relève informatique)	Plan de réponse en cas de désastre (*Disaster Recovery Plan*) ou de crise majeure, maintien des technologies essentielles aux opérations de l'organisation. Le plan anti-sinistre se distingue du plan de continuité qui adresse l'ensemble des opérations d'affaires de l'organisation.
Plan de continuité (continuité des affaires)	Plan de réponse en cas de désastre ou de crise majeure, maintien des opérations essentielles, reconstruction, relocalisation, reprise des opérations, etc. Le plan de continuité se distingue du plan anti-sinistre qui adresse uniquement la relève technologique de l'organisation.

Plan de relève informatique (voir Plan anti-sinistre)	Plan de réponse en cas de désastre (*Disaster Recovery Plan*) ou de crise majeure, maintien des technologies essentielles aux opérations de l'organisation. Le plan anti-sinistre se distingue du plan de continuité qui adresse l'ensemble des opérations d'affaires de l'organisation.
Plan de réponse aux incidents	Le plan de réponse en cas d'incident de sécurité est une méthode documentée de gestion qui est utilisé pour identifier, répondre, limiter et contrer les incidents au fur et à mesure qu'ils surviennent.
Point de contrôle	Élément physique ou logique qui contrôle l'accès d'un segment réseau à un autre. Les coupe-feux et aiguilleurs agissent habituellement comme point de contrôle réseautique. Pourront également être considérés comme « point de contrôle » les services d'authentification à deux facteurs qui valident les privilèges d'un utilisateur avant de lui octroyer l'accès à une zone du réseau de l'organisation.
Politique	Document qui sert de guide et de cadre aux décisions. Il précise le quoi, le pourquoi et les principaux intervenants. Elle est généralement approuvée par le Conseil d'Administration de l'organisation.
Positionnement	Point de vue exprimé officiellement par la sécurité de l'information sur un domaine spécifique. Il peut également s'agir d'une interprétation provisoire d'un élément d'une politique ou d'une directive en attendant que celle-ci soit mise-à-jour. Dans ce contexte, un positionnement a une valeur obligatoire similaire à une politique ou une directive de sécurité.
Pourriel	Communication électronique non sollicitée via le courrier électronique.
Principe	Dans le contexte d'une politique ou d'une directive, moyen qui, s'il est adéquatement mis en place, devrait permettre de rencontrer les objectifs visés par une mesure de sécurité.
Principe du moindre privilège	Principe de sécurité de l'information consistant en l'octroi de privilèges d'accès restreints aux seuls actifs informationnels requis pour accomplir les tâches nécessaires à l'exercice d'une fonction.
Procédure (Voir Processus)	Une procédure décrit et formalise les tâches à accomplir pour mettre en œuvre le processus. Si la procédure n'est pas respectée, les données de sorties du processus ne seront pas conformes aux exigences attendues : elle précise le quoi, le comment, le quant et les intervenants. Les procédures viennent supporter les directives. Elles sont généralement approuvées par les directions ou services concernés.

Processus (Voir Procédure)	Le processus est un ensemble d'opérations, décomposables en tâches, en vue d'un résultat déterminé. Un processus est une suite d'actions qui ne sont pas séquentielles comme l'est une procédure. Il se définit par sa nature transactionnelle: «produire X», «concevoir Y», «transporter Z de A à B», «facturer les prestations XYZ », etc. Les processus viennent supporter les directives. Elles sont généralement approuvées par les directions ou services concernés.
Propriétaire	Le propriétaire d'actifs est un gestionnaire désigné comme responsable de l'actif nécessaire à la conduite des activités de l'organisation. Les actifs sont généralement assignés aux propriétaires selon les processus d'affaires supportés.
Propriétaire délégué	Un Propriétaire délégué est un employé de l'organisation (habituellement un Directeur ou un gestionnaire) responsable d'un secteur et d'un ou plusieurs processus d'affaires. Il est désigné par le Propriétaire de l'information.
Registre de classification	Inventaire de l'ensemble des actifs informationnels classifiés. Le registre de classification est la source autoritaire de la cote DIC attribuée à un actif informationnel.
Registre de risque	Inventaire de l'ensemble des risques évalués et liés aux actifs informationnels.
Registre des incidents	Inventaire des incidents de sécurité de l'information qui documente chaque incident et la résolution de celui-ci. Le registre permet d'optimiser le processus de gestion des incidents et ainsi réduire l'occurrence et l'impact de ces-derniers.
Renseignement confidentiel (ou information confidentielle)	Tout renseignement utilisé pour la conduite des affaires de l'organisation qui n'est pas de nature publique. Les renseignements personnels sont tous des renseignements confidentiels.
Renseignement personnel	Tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresses et numéros de téléphone de son lieu de travail. (Extrait de la *Loi sur la protection des renseignements personnels et les documents électroniques*, voir https://www.priv.gc.ca/leg_c/interpretations_02_f.asp)
Renseignement personnel sensible	Renseignement personnel dont l'usage pourrait être préjudiciable à la personne en facilitant un vol d'identité. Cette catégorie comprend notamment la date de naissance, le numéro d'assurance sociale et les coordonnées bancaires.
Répertoire central d'identités	Endroit où stocker toutes les identités qui sont utilisées dans les systèmes d'information de l'organisation. A titre d'exemple, un *Active Directory* de Windows est habituellement considéré comme un répertoire central d'identité.

Responsable de la sécurité de l'information (RSI)	Désigne le gestionnaire du département de la sécurité de l'information de l'organisation.
Risque	Incidence potentielle d'un événement pouvant affecter négativement les activités de l'organisation ou nuire d'une quelconque façon à l'exécution de son mandat. L'évaluation d'un niveau de risque tient compte de la plausibilité d'un événement et de la criticité de son impact potentiel sur les actifs de l'organisation.
Risque résiduel	Risque qui subsiste suite à l'application de tous les contrôles de sécurité.
SaaS	Une solution SaaS, ou *Software as a Service*, fournit le logiciel ou l'application, regroupant les services de l'IaaS et du PaaS avec en plus, l'installation, la maintenance et la configuration comprises. C'est une interface qui permet la simple utilisation du logiciel et ne nécessite pas de connaissance informatique ou technique au préalable. Les logiciels SaaS sont souvent sous forme d'abonnements mensuels.
Salle informatique	Local fermé et aménagé spécifiquement pour y stocker et y opérer des environnements informatiques tout en fournissant un environnement contrôlé qui limite certains risques d'interruptions ou de mauvais fonctionnements.
Sécurité de l'information (Voir cybersécurité)	Protection de la confidentialité, de l'intégrité et de la disponibilité de l'information. L'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées. A la différence du terme "Cybersécurité", celui-ci regroupe tous les formats d'informations qu'ils soient papier, numériques ou autres.
Sécurité physique	Contrôle du périmètre, contrôle d'accès, surveillance, gardiennage, protection contre les incendies et matières dangereuses, etc.
Services externalisés ou hébergés (Voir Services impartis)	Transfert de tout ou partie d'une fonction informatique de l'organisation vers un partenaire externe.
Seuil de tolérance aux risques	Seuil d'acceptabilité du risque au-delà duquel le risque doit être adressé.
Signature numérique	Mécanisme permettant de garantir l'intégrité d'un document électronique et d'en authentifier l'auteur, par analogie avec la signature manuscrite d'un document papier.
Standard	Les standards sont une description de bas niveau de la manière dont l'organisation appliquera sa stratégie en matière de sécurité de l'information. En d'autres termes, ils sont utilisés pour maintenir un niveau minimum de sécurité efficace.

Supports amovibles	Les supports amovibles comprennent les disques de mémoire flash, les disques durs amovibles, les CD, les DVD et les supports imprimés.
Surveillance	Signifie toute activité permettant de détecter les vulnérabilités et les intrusions affectant les réseaux, les serveurs, les applications, les banques d'informations et les Actifs informationnels.
Système d'exploitation	Un système d'exploitation (*Operating System* ou OS) est un ensemble de programmes spécialisés qui permet l'utilisation des ressources matérielles d'un ordinateur.
Système d'information	Terme générique servant à désigner tout système servant à traiter ou transmettre de l'information. Cette expression comprend notamment : logiciels et programmes, ordinateur fixe, ordinateur portable, système téléphonique, bloc-notes numérique, appareils intelligents (ex. : tablette, cellulaire, etc.), équipements réseautiques, imprimante et autres périphériques, support de données tel que clés USB, disque dur externe et tout autre outil informatique (matériel ou logiciel) pouvant être utilisé par le personnel de l'organisation. Aux fins des encadrements de l'organisation, un Système d'information externalisé (Saas, IaaS, PaaS) est considéré comme un système interne à l'organisation.
Système d'information personnel (voir Appareil personnel)	Tout système d'information fourni par l'utilisateur, par opposition aux systèmes d'information fourni par l'employeur.
Techniquement possible	Expression utilisée pour qualifier le caractère impératif d'un requis de sécurité. Le requis n'est pas applicable de manière absolue mais seulement si les technologies en place permettent son application.
Technologie de l'information	Ensemble des équipements, logiciels et services utilisés pour la collecte, le traitement et la transmission des Actifs informationnels.
Télétravail	Toute forme d'organisation du travail dans laquelle une activité qui normalement serait exécutée dans les locaux de l'organisation est réalisée par un *Employé* ou un *Consultant* hors de ces locaux en utilisant les technologies de l'information à l'aide d'équipements fournis et/ou géré par l'organisation ou autres équipements autorisés par l'organisation.
Tests d'intrusion	Activité administrative ou technique autorisée et planifiée qui permet de simuler une attaque par une entité malveillante à l'égard d'un actif informationnel. Les tests d'intrusion visent essentiellement à vérifier l'efficacité des contrôles de sécurité en place.
Utilisateur	Toute personne qui utilise des actifs informationnels de l'organisation, incluant mais ne se limitant pas aux employés, stagiaires, consultants ou fournisseurs.

Virus (voir code malveillant, logiciel malveillant, *malware*)	Un virus ou logiciel malveillant (de l'anglais malware) est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté. De nos jours, le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les maliciels englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.
Visiteur	Désigne toute personne, autre qu'un employé, ayant besoin d'entrer dans les locaux d'un établissement pour une courte période, habituellement moins d'une journée.
Vol d'identité	Se produit lorsqu'une personne obtient et utilise des renseignements personnels d'une tierce personne afin de lui imputer des actions.
Vulnérabilité	Faiblesse dans un système d'information permettant à une menace de porter atteinte à l'intégrité de ce système, à son fonctionnement normal (sa disponibilité) où à la confidentialité des informations qu'il contient.