Norme Marocaine

NM ISO/CEI 27002

2009

(Indice de classement 00.5.702)

Technologies de l'information

Techniques de sécurité

Code de bonne pratique pour la gestion de la sécurité de l'information

Norme Marocaine homologuée

Par arrêté du Ministre de l'Industrie, du Commerce et des Nouvelles Technologies N° du , publié au B.O. N° du

Correspondance

La présente norme reprend intégralement la norme ISO/CEI 27002/2005 et son A1/2007.

Modifications

Examinée et adoptée par le comité technique de normalisation des des systèmes de management
Editée et diffusée par le Service de Normalisation Industrielle Marocaine (SNIMA)

ICS : 35.040

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27002 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

La première édition de l'ISO/CEI 27002 comprend l'ISO/CEI 17799:2005 et l'ISO/CEI 17799:2005/Cor.1:2007. Son contenu technique est identique à celui de l'ISO/CEI 17799:2005. L'ISO/CEI 17799:2005/Cor.1:2007 modifie le numéro de référence de la norme de 17799 en 27002. L'ISO/CEI 17799:2005 et l'ISO/CEI 17799:2005/Cor.1:2007 sont provisoirement retenus jusqu'à la publication de la deuxième édition de l'ISO/CEI 27002.

NORME INTERNATIONALE ISO/CEI 17799:2005
RECTIFICATIF TECHNIQUE 1

Publié 2007-07-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information

RECTIFICATIF TECHNIQUE 1

Information technology — Security techniques — Code of practice for information security management

TECHNICAL CORRIGENDUM 1

Le Rectificatif technique 1 à l'ISO/CEI 17799:2005 a été élaboré par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Dans tout le document:

Remplacer «17799» par «27002».

ICS 35.040 **Réf. nº ISO/CEI 17799:2005/Cor.1:2007(F)**

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 17799 a été élaborée par le comité technique ISO/TC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette deuxième édition annule et remplace la première édition (ISO/CEI 17799:2000), qui a fait l'objet d'une révision technique. À l'inverse de la version anglaise, la version française ne comporte pas d'Index.

Une famille de Normes internationales concernant le système de gestion de la sécurité de l'information (ISMS, de Information Security Management System) est en préparation au sein de l'ISO/CEI JTC 1/SC 27. La famille inclut des Normes internationales relatives aux exigences du système de gestion de la sécurité de l'information, à la gestion du risque, à la métrologie et au mesurage, ainsi qu'à un guide de mise en application. La famille adoptera un schéma de numérotation utilisant la série des nombres 27000 et suivants.

À partir de 2007, il est proposé d'incorporer la nouvelle édition de l'ISO/CEI 17799 dans ce schéma de numérotation en tant qu'ISO/CEI 27002.

0 Introduction

0.1 Qu'est-ce que la sécurité de l'information ?

L'information constitue un bien important pour l'organisme; elle est à ce titre un élément important de l'activité de l'organisme et elle nécessite une protection adéquate. Ce point s'avère particulièrement important dans l'environnement actuel qui comporte des interconnexions de plus en plus nombreuses. Du fait du nombre croissant de ces interconnexions, l'information est de plus en plus exposée et vulnérable (voir également les lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information).

L'information se présente sur des supports variés. Elle peut être disponible sur papier, stockée électroniquement, transmise par voie postale ou électronique, diffusée sur des supports audiovisuels ou verbalement. Quel que soit le support ou le moyen utilisé pour la partager ou la stocker, il convient de toujours protéger l'information de manière adaptée.

La sécurité de l'information vise à protéger l'information contre une large gamme de menaces, de manière à garantir la continuité des transactions, à réduire le plus possible le risque et à optimiser le retour sur investissement ainsi que les opportunités en termes d'activité pour l'organisme.

La sécurité de l'information est assurée par la mise en œuvre de mesures adaptées, qui regroupent des règles, des processus, des procédures, des structures organisationnelles, et des fonctions matérielles et logicielles. Ces mesures doivent être spécifiées, mises en œuvre, suivies, réexaminées et améliorées aussi souvent que nécessaire, de manière à atteindre les objectifs spécifiques en matière de sécurité et d'activité d'un organisme. Pour ce faire, il convient d'agir de manière concertée avec les autres processus de gestion de l'organisme.

0.2 En quoi la sécurité de l'information est-elle nécessaire ?

L'information et les processus, systèmes et réseaux qui en permettent le traitement constituent des biens importants pour un organisme. Il peut s'avérer crucial de définir, réaliser, entretenir et améliorer la sécurité de l'information pour faire face à la concurrence, maintenir les liquidités, la rentabilité, la mise en conformité avec la loi et l'image commerciale.

Les menaces qui pèsent sur les organismes et leurs systèmes et réseaux d'information sont d'origines très diverses: fraude informatique, espionnage, sabotage, vandalisme, incendies ou inondations par exemple. Des techniques d'attaque comme les codes malveillants, le piratage informatique et les attaques par déni de service deviennent de plus en plus répandues et sophistiquées.

La sécurité de l'information revêt de l'importance pour les organismes des secteurs public et privé, et permet de protéger les infrastructures critiques. Dans ces deux secteurs, la sécurité de l'information fait office d'activateur. En d'autres termes, elle rend possible l'administration ou le commerce en ligne, et permet d'éviter le risque qui en découle ou d'en réduire l'impact. L'interconnexion des réseaux public et privé, ainsi que le partage des sources d'information, rendent le contrôle d'accès plus difficile. Le développement de l'informatique distribuée a également affaibli l'efficacité du contrôle spécialisé et centralisé.

De nombreux systèmes d'information ont été spécifiés sans que soient pris en compte les besoins de sécurité. La sécurité qui peut être mise en œuvre par des moyens techniques est limitée et il convient de la prendre en charge à l'aide de moyens de gestion et de procédures adaptés. Pour identifier les mesures à mettre en place, il convient de procéder à une planification minutieuse et de prêter attention aux détails. La participation de tous les salariés d'un organisme est indispensable à une bonne gestion de la sécurité de l'information. La participation des actionnaires, des fournisseurs, des tiers, des clients et autres peut également s'avérer nécessaire. De même, l'avis de spécialistes tiers peut être également nécessaire.

0.3 Définition des exigences en matière de sécurité

Un organisme doit impérativement identifier ses exigences en matière de sécurité. Ces exigences proviennent de trois sources principales.

1. La première est l'appréciation du risque propre à l'organisme, en prenant en compte la stratégie et les objectifs généraux de l'organisme. L'appréciation du risque permet d'identifier les menaces pesant sur les biens, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel.

2. La deuxième concerne, d'une part, les exigences légales, statutaires, réglementaires, et contractuelles auxquelles l'organisme et ses partenaires commerciaux, contractants et prestataires de service, doivent répondre et, d'autre part, l'environnement socioculturel.

3. La troisième correspond à l'ensemble de principes, d'objectifs et d'exigences métier en matière de traitement de l'information que l'organisme s'est constitués pour mener à bien ses activités.

0.4 Appréciation du risque lié à la sécurité

Les exigences en matière de sécurité sont identifiées par une évaluation méthodique des risques. Les dépenses consacrées aux mesures et les dommages susceptibles de résulter de défaillances de la sécurité doivent être mis en perspective.

Les résultats de l'appréciation du risque permettent de définir les actions de gestion appropriées et les priorités en matière de management du risque, et d'identifier les mesures adaptées destinées à contrer ces risques.

Il convient de procéder régulièrement à l'appréciation du risque, afin de tenir compte de toute modification pouvant influer les résultats de l'analyse.

Pour plus ample information sur l'appréciation du risque lié à la sécurité, voir 4.1 «Appréciation du risque lié à la sécurité».

0.5 Sélection des mesures

Lorsque les exigences et les risques liés à la sécurité ont été identifiés, et que les décisions de traitement des risques ont été prises, il convient de sélectionner et de mettre en œuvre des mesures appropriées, afin de ramener les risques à un niveau acceptable. Selon les cas, il est possible de sélectionner les mesures dans la présente norme ou dans d'autres guides, ou encore de spécifier de nouvelles mesures en vue de satisfaire des besoins spécifiques. La sélection des mesures de sécurité dépend des décisions prises par l'organisme en fonction de ses critères d'acceptation du risque, de ses options de traitement du risque, et de son approche du management général du risque. Il convient également de prendre en considération les lois et règlements nationaux et internationaux concernés.

Certaines mesures décrites dans la présente norme peuvent être considérées comme des principes directeurs pour la gestion de la sécurité de l'information et être appliquées à la plupart des organismes. Elles sont détaillées ci-après, sous le titre «Bases de la sécurité de l'information».

Pour plus ample information sur la sélection des mesures et les options de traitement du risque, voir 4.2 «Traitement du risque lié à la sécurité».

0.6 Bases de la sécurité de l'information

Une base solide pour aborder la sécurité de l'information est constituée des mesures suivantes, provenant d'exigences légales essentielles, ou considérées comme faisant partie de la pratique courante dans le domaine de la sécurité de l'information.

Les mesures jugées cruciales pour un organisme d'un point de vue légal concernent, selon la législation en vigueur, les aspects suivants:

a) la protection des données et la confidentialité des informations relatives à la vie privée (voir 15.1.4);

b) la conservation des enregistrements de l'organisme (voir 15.1.3);

c) les droits de propriété intellectuelle (voir 15.1.2).

Les mesures considérées comme faisant partie de la pratique courante en matière de sécurité de l'information portent sur les points suivants:

a) le document de politique de sécurité de l'information (voir 5.1.1);

b) l'affectation des responsabilités en matière de sécurité de l'information (voir 6.1.3);

c) la sensibilisation, la qualification et la formation relatives à la sécurité de l'information (voir 8.2.2);

d) le traitement correct de l'information dans les applications (voir 12.2);

e) la gestion des vulnérabilités (voir 12.6);

f) la gestion de la continuité de l'activité (voir Article 14);

g) la gestion des incidents et de l'amélioration de la sécurité de l'information (voir 13.2).

Ces mesures s'appliquent à la plupart des organismes et des environnements.

Toutes les mesures décrites dans la présente norme présentent de l'importance et il convient de les prendre en compte. Cependant, il convient de déterminer la pertinence de chacune en fonction des risques spécifiques auxquels l'organisme est exposé. Par conséquent, bien que l'approche ci-dessus soit considérée comme une base solide, elle ne remplace pas la sélection de mesures reposant sur une évaluation du risque.

0.7 Facteurs cruciaux de réussite

L'expérience montre que les facteurs suivants s'avèrent souvent cruciaux lors de la mise en œuvre de la sécurité de l'information au sein d'un organisme:

a) une politique, des objectifs et des activités relatives à la sécurité de l'information cohérents avec les objectifs d'activité de l'organisme;

b) une approche et un système de mise en œuvre, d'entretien, de suivi et d'amélioration de la sécurité de l'information conforme avec la culture de l'organisme;

c) le soutien et l'engagement visibles de tous les niveaux de la direction;

d) une bonne compréhension des exigences en matière de sécurité de l'information, d'évaluation et de gestion des risques;

e) une communication efficace sur la sécurité de l'information auprès de tous les responsables, salariés et autres parties, afin de les sensibiliser sur le sujet;

f) la diffusion des lignes directrices sur la politique et les normes de sécurité de l'information auprès de tous les responsables, salariés et autres parties;

g) la mise en place d'un budget dévolu aux activités de gestion de la sécurité de l'information;

h) la définition de mesures adéquates pour la sensibilisation, la qualification et la formation;

i) la mise en place d'un processus performant de gestion des incidents liés à la sécurité de l'information;

j) la mise en œuvre d'un système de mesures[1)] afin d'évaluer les performances de l'organisation en matière de gestion de la sécurité, et de fournir des orientations d'amélioration du système.

0.8 Mise au point des lignes directrices propres à l'organisme

Ce code de bonne pratique peut servir de base pour la mise au point de lignes directrices spécifiques à un organisme. Une partie des mesures et lignes directrices de ce code de bonne pratique peut n'être pas nécessaire ou adapté. Par ailleurs, des mesures et des lignes directrices ne figurant pas dans la présente norme peuvent être nécessaires. Lors de la rédaction de documents contenant des lignes directrices ou des mesures supplémentaires, il pourra être utile d'intégrer des références croisées aux articles de la présente norme, le cas échéant, afin de faciliter la vérification de la conformité par les auditeurs et les partenaires commerciaux.

1) Il est important de noter que le mesurage de la sécurité de l'information dépasse le domaine d'application de la présente Norme internationale.

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour la gestion de la sécurité de l'information

1 Domaine d'application

La présente Norme internationale établit des lignes directrices et des principes généraux pour préparer, mettre en œuvre, entretenir et améliorer la gestion de la sécurité de l'information au sein d'un organisme. Les objectifs esquissés dans la présente Norme internationale fournissent une orientation générale sur les buts acceptés communément dans la gestion de la sécurité de l'information.

Les objectifs et mesures décrits dans la présente Norme internationale sont destinés à être mis en œuvre pour répondre aux exigences identifiées par une évaluation du risque. La présente Norme internationale est prévue comme base commune et ligne directrice pratique pour élaborer les référentiels de sécurité de l'organisation, mettre en œuvre les pratiques efficaces de la gestion de la sécurité, et participer au développement de la confiance dans les activités entre organismes.

2 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

2.1
bien
«asset»
tout élément représentant de la valeur pour l'organisme

[ISO/CEI 13335-1:2004]

2.2
mesure
«control»
moyen de gérer un risque, comprenant la politique, les procédures, les lignes directrices, et les pratiques ou structures organisationnelles, et pouvant être de nature administrative, technique, gestionnaire ou juridique

NOTE Le terme «mesure» est également utilisé comme synonyme de «conservation» ou de «contre-mesure».

2.3
ligne directrice
description clarifiant ce qu'il convient de réaliser et par quels moyens, en vue d'atteindre les objectifs fixés par la politique de l'organisme

[ISO/CEI 13335-1:2004]

2.4
moyens de traitement de l'information
tout(e) système, service ou infrastructure de traitement de l'information, ou locaux les abritant

2.5
sécurité de l'information
protection de la confidentialité, de l'intégrité et de la disponibilité de l'information; en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées

2.6
événement lié à la sécurité de l'information
occurrence identifiée d'un état d'un système, d'un service ou d'un réseau, indiquant une brèche possible dans la politique de sécurité de l'information ou un échec des moyens de protection, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité

[ISO/CEI TR 18044:2004]

2.7
incident lié à la sécurité de l'information
un incident lié à la sécurité de l'information est indiqué par un ou plusieurs événement(s) de sécurité de l'information indésirable(s) ou inattendu(s) présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information

[ISO/CEI TR 18044:2004]

2.8
politique
intentions et dispositions générales formellement exprimées par la direction

2.9
risque
combinaison de la probabilité d'un événement et de ses conséquences

[ISO/CEI Guide 73:2002]

2.10
analyse du risque

utilisation systématique d'informations pour identifier les sources et pour estimer le risque

[ISO/CEI Guide 73:2002]

2.11
appréciation du risque

ensemble du processus d'analyse du risque et d'évaluation du risque

[ISO/CEI Guide 73:2002]

2.12
évaluation du risque
processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l'importance d'un risque

[ISO/CEI Guide 73:2002]

2.13
management du risque
activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque

NOTE Le management du risque inclut généralement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque.

[ISO/CEI Guide 73:2002]

2.14
traitement du risque
processus de sélection et de mise en œuvre des mesures visant à modifier le risque

[ISO/CEI Guide 73:2002]

2.15
tiers
personne ou organisme reconnu(e) comme indépendant(e) des parties concernées

2.16
menace
cause potentielle d'un incident indésirable, pouvant entraîner des dommages au sein d'un système ou d'un organisme

[ISO/CEI 13335-1:2004]

2.17
vulnérabilité
faiblesse d'un bien ou d'un groupe de biens pouvant faire l'objet d'une menace

[ISO/CEI 13335-1:2004]

3 Structure de la présente Norme internationale

La présente Norme internationale contient 11 articles relatifs aux mesures de sécurité, qui comprennent un total de 39 catégories de sécurité et un article d'introduction sur l'appréciation et le traitement du risque.

3.1 Articles

Chaque article contient plusieurs catégories de sécurité principales. Les 11 articles (accompagnés du nombre de catégories de sécurité principales incluses dans chaque article) sont les suivants.

a) Politique de sécurité (1).

b) Organisation de la sécurité de l'information (2).

c) Gestion des biens (2).

d) Sécurité liée aux ressources humaines (3).

e) Sécurité physique et environnementale (2).

f) Gestion opérationnelle et gestion de la communication (10).

g) Contrôle d'accès (7).

h) Acquisition, développement et maintenance des systèmes d'information (6).

i) Gestion des incidents liés à la sécurité de l'information (2).

j) Gestion de la continuité de l'activité (1).

k) Conformité (3).

NOTE L'ordre de classement des articles dans la présente norme n'est aucunement lié à leur importance. Selon les circonstances, tous les articles peuvent être importants; par conséquent, il convient que chaque organisme appliquant la présente norme identifie les articles appropriés, l'importance de chacun et l'application de ces articles aux processus métier cibles. Plus généralement, les listes contenues dans la présente norme ne sont pas classées par ordre de priorité, sauf indication contraire.

3.2 Principales rubriques

Chaque rubrique principale de sécurité comprend

a) un objectif de sécurité identifiant le but à atteindre, et

b) une ou plusieurs mesure(s) pouvant être appliquée(s) en vue d'atteindre l'objectif de sécurité.

La description des mesures est structurée de la manière suivante:

Mesure

Spécifie la mesure adaptée à l'objectif de sécurité.

Préconisations de mise en œuvre

Propose des informations détaillées pour mettre en œuvre la mesure et pour atteindre l'objectif de sécurité. Il se peut que certaines préconisations ne soient pas adaptées à tous les cas et que d'autres solutions s'avèrent préférables.

Informations supplémentaires

Présente des compléments d'information à considérer, par exemple des éléments juridiques et des références à d'autres normes.

4 Appréciation et traitement du risque

4.1 Appréciation du risque lié à la sécurité

Il convient de réaliser une analyse du risque de manière à identifier, quantifier et affecter des priorités aux risques en fonction des critères d'acceptation et des objectifs fixés par l'organisme. Il convient que les résultats de l'appréciation du risque permettent de définir de façon pertinente les actions à engager et les priorités en matière de management du risque lié à la sécurité de l'information, et facilitent le choix des mesures appropriées destinées à protéger l'information contre ce risque. Il peut être nécessaire de répéter le processus d'appréciation du risque et de sélection des mesures en vue de couvrir les différentes composantes de l'organisme ou des systèmes d'information.

Il convient que l'appréciation du risque prévoie l'évaluation systématique de l'ampleur du risque (analyse du risque) et la comparaison des risques estimés par rapport au niveau de risque acceptable, afin de déterminer l'importance du risque (évaluation du risque).

Il convient de réaliser régulièrement une appréciation du risque afin de prendre en compte les modifications des exigences de sécurité et de l'exposition au risque, par exemple: biens, menaces, vulnérabilités, impacts, évaluation du risque et moments auxquels des modifications importantes interviennent. Il convient d'effectuer cette appréciation du risque de manière méthodique afin d'obtenir des résultats comparables et reproductibles.

Pour être efficace, il convient de clairement définir le domaine d'application de l'appréciation du risque. Il convient également de mettre en place des relations avec les appréciations du risque d'autres domaines, le cas échéant.

Le domaine d'application peut concerner tout ou partie d'un organisme, un système d'information, des composants système spécifiques ou des services pour lesquels une appréciation du risque est réalisable et

utile. Des exemples de méthodologies d'appréciation du risque sont présentés dans l'ISO/CEI TR 13335-3, *Technologies de l'information — Lignes directrices pour la gestion de sécurité IT —Partie 3: Techniques pour la gestion de sécurité IT*.

4.2 Traitement du risque lié à la sécurité

Avant d'envisager le traitement d'un risque, il convient que l'organisme décide des critères permettant de déterminer si le risque est acceptable ou non. Ils le sont si par exemple l'appréciation a révélé que le risque est faible ou que le coût du traitement s'avère faible pour l'organisme. Il convient d'enregistrer de telles décisions.

Pour chacun des risques identifiés à l'issue de la phase d'appréciation du risque, une décision relative au traitement du risque doit être prise. Les solutions envisageables sont les suivantes:

a) application de mesures appropriées visant à réduire le risque;

b) acceptation des risques en connaissance de cause et avec objectivité, dans la mesure où ils sont acceptables au regard de la politique de l'organisme et des critères d'acceptation;

c) annulation des risques en interdisant les actions susceptibles de les engendrer;

d) transfert des risques à des tiers, par exemple assureurs et fournisseurs.

Lorsque la décision du traitement du risque consiste à appliquer des mesures appropriées, il convient de sélectionner et de mettre en œuvre ces mesures en fonction des exigences identifiées par une appréciation du risque. Il convient que les mesures garantissent une réduction du risque à un niveau acceptable, en tenant compte des éléments suivants:

a) exigences et contraintes de la législation et de la réglementation nationales et internationales;

b) objectifs de l'organisme;

c) exigences et contraintes opérationnelles;

d) coût de mise en œuvre et d'exploitation des mesures par rapport à la réduction du risque, tout en respectant les exigences et les contraintes de l'organisme;

e) nécessité d'équilibrer l'investissement que représentent la mise en œuvre et l'exploitation des mesures par rapport aux dommages potentiels dus à des failles de sécurité.

Selon les cas, il est possible de sélectionner les mesures dans la présente norme ou dans d'autres guides, ou encore de spécifier de nouvelles mesures en vue de satisfaire des besoins spécifiques. Il est important de noter que certaines mesures ne s'appliquent pas à tous les systèmes d'information ou environnements, ou ne sont pas adaptées à toutes les organisations. À titre d'exemple, il est décrit en 10.1.3 comment cloisonner les tâches afin de prévenir la fraude et les erreurs. Il peut s'avérer impossible de séparer toutes les tâches pour les petites structures; il est alors nécessaire de concevoir d'autres méthodes pour atteindre le même objectif de sécurité. Un autre exemple, donné en 10.10, décrit comment surveiller l'utilisation d'un système et recueillir des preuves. Les mesures préconisées, par exemple la journalisation des événements, peuvent être inadaptées si elles entrent en conflit avec la législation en vigueur, telle que le respect de la vie privée des clients ou des collaborateurs.

Il convient d'envisager la mise en place de mesures de sécurité dès les phases de conception et de spécification des systèmes et des projets; une prise en compte tardive de la problématique sécurité peut entraîner des surcoûts, conduire à des solutions moins pertinentes, voire à l'incapacité d'atteindre un niveau de sécurité satisfaisant.

Il convient de garder à l'esprit qu'aucune série de mesures ne peut assurer une sécurité totale et qu'il convient d'engager des actions supplémentaires pour surveiller, évaluer et améliorer l'efficacité des mesures de sécurité.

5 Politique de sécurité

5.1 Politique de sécurité de l'information

Objectif: Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.

Il convient que la direction définisse des dispositions générales claires en accord avec ses objectifs et qu'elle démontre son soutien et son engagement vis-à-vis de la sécurité de l'information en mettant en place et maintenant une politique de sécurité de l'information pour tout l'organisme.

5.1.1 Document de politique de sécurité de l'information

Mesure

Il convient qu'un document de politique de sécurité de l'information soit approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.

Préconisations de mise en œuvre

Il convient que le document de politique de sécurité de l'information démontre l'engagement de la direction et définisse l'approche de l'organisme pour gérer la sécurité de l'information. Il convient que ce document de politique contienne les éléments suivants:

a) une définition de la sécurité de l'information, les objectifs généraux recherchés et le domaine d'application retenu, ainsi que l'importance de la sécurité en tant que mécanisme nécessaire au partage de l'information (voir Introduction);

b) une déclaration des intentions de la direction soutenant les objectifs et principes de la sécurité de l'information, en conformité avec la stratégie et les objectifs de l'organisme;

c) une démarche de définition des objectifs de sécurité et des mesures, intégrant l'appréciation et le management du risque;

d) une brève explication des politiques, principes, normes et exigences en matière de conformité qui présentent une importance particulière pour l'organisme, à savoir les éléments suivants:

   1) la conformité avec les exigences légales, réglementaires et contractuelles;

   2) les exigences en terme de formation et de sensibilisation en matière de sécurité;

   3) la gestion de la continuité de l'activité;

   4) les conséquences des violations de la sécurité de l'information;

e) une définition des responsabilités générales et spécifiques dans le domaine de la gestion de la sécurité de l'information, traitant en particulier de la remontée d'incidents de sécurité;

f) des références à la documentation susceptible d'appuyer la politique et devant être respectée, par exemple des politiques et des procédures de sécurité plus détaillées ou des règles de sécurité devant être respectées par les usagers.

Il convient de communiquer cette politique de sécurité de l'information à l'ensemble des utilisateurs sous une forme adéquate, accessible et compréhensible pour les destinataires.

Informations supplémentaires

La politique de sécurité de l'information peut éventuellement faire partie d'un document de politique générale. Si la politique de sécurité de l'information est diffusée hors de l'organisme, il convient de veiller à ne pas divulguer d'informations sensibles. Pour plus ample information, voir l'ISO/CEI 13335-1:2004.

5.1.2 Réexamen de la politique de sécurité de l'information

Mesure

Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, il convient de réexaminer la politique à intervalles fixés préalablement ou en cas de changements majeurs.

Préconisations de mise en œuvre

Il convient qu'une personne soit désignée comme responsable de la politique de sécurité de l'information, mandatée par la direction pour développer, réexaminer et évaluer cette politique. Il convient que le réexamen permette une appréciation des possibilités d'amélioration de la politique de sécurité de l'information de l'organisme, et une approche de gestion de la sécurité de l'information compte tenu des changements intervenant dans l'environnement organisationnel, des circonstances liées à l'activité, des conditions légales ou de l'environnement technique.

Il convient que le réexamen de la politique de sécurité de l'information tienne compte des revues de gestion. Il convient de définir des procédures de revues de gestion, notamment un calendrier ou une période de revue.

En entrée des revues de gestion, il convient que les informations suivantes soient disponibles:

a) un retour des parties intéressées;

b) les résultats de revues indépendantes (voir 6.1.8);

c) l'état des actions préventives et correctives (voir 6.1.8 et 15.2.1);

d) les résultats des précédentes revues de gestion;

e) la conformité avec les exigences de performances du processus et la politique de sécurité de l'information;

f) les changements pouvant avoir une incidence sur l'approche de l'organisme en matière de gestion de la sécurité de l'information, par exemple les changements dans l'environnement organisationnel, les circonstances propres à l'activité, la disponibilité des ressources, les conditions contractuelles, réglementaires et légales ou l'environnement technique;

g) les tendances relatives aux menaces et à la vulnérabilité;

h) les incidents de sécurité remontés (voir 13.1);

i) les recommandations émanant des autorités compétentes (voir 6.1.6).

Il convient que les résultats des revues de gestion définissent les décisions et les actions relatives aux aspects suivants:

a) l'amélioration de l'approche de l'organisme en matière de gestion de la sécurité et des processus supports;

b) l'amélioration des objectifs de sécurité et des mesures;

c) l'amélioration de l'affectation des ressources et/ou des responsabilités.

Il convient de tenir à jour un enregistrement des revues.

Une fois révisée, il convient que la politique de sécurité soit approuvée par la direction.

6 Organisation de la sécurité de l'information

6.1 Organisation interne

Objectif: gérer la sécurité de l'information au sein de l'organisme.

Il convient d'établir un cadre de gestion pour initialiser, puis contrôler la mise en œuvre de la sécurité de l'information au sein de l'organisme.

Il convient que la direction approuve la politique de sécurité de l'information, attribue les rôles liés à la sécurité, puis coordonne et réexamine la mise en œuvre de la sécurité à travers l'organisme.

Si nécessaire, il convient de créer un pôle de conseil spécialisé dans le domaine de la sécurité de l'information et de le mettre à la disposition de tous dans l'organisme. Il convient de développer des contacts avec des spécialistes externes de la sécurité, y compris avec les autorités compétentes, afin de suivre les tendances industrielles et les méthodes d'appréciation existantes, de mettre en place une veille normative et de créer des points de contact adaptés au traitement d'incidents liés à la sécurité de l'information. Il convient de favoriser une approche multidisciplinaire de la sécurité de l'information.

6.1.1 Engagement de la direction vis-à-vis de la sécurité de l'information

Mesure

Il convient que la direction soutienne activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement franc, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.

Préconisations de mise en œuvre

Il convient que la direction

a) garantisse que les objectifs concernant la sécurité de l'information sont identifiés, répondent aux besoins de l'organisme et soient intégrés dans des processus adaptés,

b) formule, revoie et approuve la politique de sécurité de l'information,

c) contrôle l'efficacité de la mise en œuvre de la politique de sécurité de l'information,

d) formule des directives claires et manifeste clairement son soutien vis-à-vis des initiatives prises pour renforcer la sécurité,

e) fournisse les ressources nécessaires à la sécurité de l'information,

f) approuve l'attribution de fonctions et de responsabilités spécifiques à la sécurité de l'information au sein de l'organisme,

g) lance des plans et des programmes visant à maintenir à niveau la sensibilisation à la sécurité de l'information, et

h) garantisse la coordination des mesures en matière de sécurité de l'information mises en œuvre au sein de l'organisme (voir 6.1.2).

Il convient que la direction identifie ses besoins en conseils (internes ou externes) en matière de sécurité de l'information, contrôle les résultats de ces conseils, puis coordonne leur application au sein de l'organisme.

Suivant la taille de l'organisme, de telles responsabilités peuvent être assumées par un comité de gestion dédié ou par un organe de direction existant, tel que le conseil d'administration.

Informations supplémentaires

Pour plus ample information, voir l'ISO/CEI 13335-1:2004.

6.1.2 Coordination de la sécurité de l'information

Mesure

Il convient que les activités relatives à la sécurité de l'information soient coordonnées par des intervenants ayant des fonctions et des rôles appropriés représentatifs des différentes parties de l'organisme.

Préconisations de mise en œuvre

De manière générale, la coordination de la sécurité de l'information repose sur la coopération et la collaboration des directeurs, des utilisateurs, des administrateurs, des développeurs d'applications, des auditeurs et du personnel chargé de la sécurité, ainsi que de spécialistes en assurance, problèmes juridiques, ressources humaines, informatique ou management du risque. Il convient que cette coordination

a) garantisse une exécution des activités liées à la sécurité conforme à la politique de sécurité de l'information,

b) définisse le mode de traitement des non-conformités aux règles,

c) approuve les méthodologies et les processus relatifs à la sécurité de l'information, tels que l'appréciation du risque et la classification des informations,

d) identifie les changements majeurs en terme de menaces, ainsi que l'exposition des informations et des processus de traitement aux menaces,

e) évalue l'adéquation des mesures de sécurité de l'information et coordonne leur mise en œuvre,

f) encourage efficacement la formation et la sensibilisation en matière de sécurité de l'information dans l'organisme, et

g) évalue les informations remontant de la surveillance et du contrôle des incidents de sécurité et émette des recommandations quant aux actions à engager en réponse à de tels incidents.

Si un groupe représentatif des différentes parties de l'organisme n'a pas pu être mis en place, par exemple parce qu'un tel groupe n'a pas lieu d'être compte tenu de la taille l'organisme, il convient que les actions décrites ci-avant soient entreprises par un autre organe de direction ou un autre responsable.

6.1.3 Attribution des responsabilités en matière de sécurité de l'information

Mesure

Il convient de définir clairement toutes les responsabilités en matière de sécurité de l'information.

Préconisations de mise en œuvre

Il convient d'attribuer les responsabilités en matière de sécurité de l'information conformément à la politique de sécurité de l'information (voir Article 4). Il convient d'identifier clairement les responsabilités quant à la protection des biens individuels et quant à l'application de processus de sécurité spécifiques. Le cas échéant, il convient de compléter ces responsabilités de directives détaillées, appropriées à certains sites et moyens de traitement de l'information. Il convient de définir clairement les responsabilités locales relatives à la protection des biens et à l'application de processus de sécurité spécifiques, comme la planification de la continuité de l'activité.

Les personnes responsables de la sécurité peuvent déléguer des tâches de sécurité. Néanmoins, elles demeurent responsables et il convient qu'elles s'assurent de la bonne mise en œuvre de chaque tâche.

Il convient de définir clairement les domaines de responsabilité de chacun et notamment de prendre les mesures suivantes:

a) il convient d'identifier et de définir clairement les biens et les processus de sécurité associés à chaque système;

b) il convient d'identifier l'entité responsable de chaque bien ou processus et de documenter sa responsabilité (voir également 7.1.2);

c) il convient de clairement définir et documenter les différents niveaux d'autorisation.

Informations supplémentaires

Dans de nombreux organismes, un responsable de la sécurité de l'information est nommé responsable de l'élaboration et de la mise en œuvre de la politique de sécurité et de la définition des mesures.

Cependant, la mise en place des ressources et des mesures reste bien souvent l'affaire d'autres managers. Une pratique courante consiste à nommer, pour chaque bien, un propriétaire qui devient alors responsable de la protection quotidienne de ce bien.

6.1.4 Système d'autorisation concernant les moyens de traitement de l'information

Mesure

Il convient de définir et de mettre en œuvre un système de gestion des autorisations pour chaque nouveau moyen de traitement de l'information.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes pour le système de gestion des autorisations:

a) il convient de doter chaque nouveau moyen de traitement de l'information d'un système approprié de gestion des autorisations selon sa finalité et son utilisation. Il convient également d'obtenir les autorisations auprès du responsable local de la sécurité du système d'information, afin de garantir le respect de l'ensemble des politiques et exigences spécifiques en matière de sécurité;

b) le cas échéant, il convient de contrôler le matériel et les logiciels en vue de garantir leur compatibilité avec les autres composants du système;

c) l'utilisation, à des fins professionnelles, d'équipements personnels ou d'usage privé, tels qu'ordinateurs portables, ordinateurs domestiques ou terminaux de poche, peut induire de nouvelles vulnérabilités; il convient alors d'identifier et de mettre en œuvre des mesures adaptées.

6.1.5 Engagements de confidentialité

Mesure

Il convient d'identifier et de réexaminer régulièrement les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisme.

Préconisations de mise en œuvre

Il convient que les modalités des engagements de confidentialité ou de non-divulgation soient exécutoires. Pour identifier les exigences en matière de confidentialité et de non-divulgation, il convient de tenir compte des éléments suivants:

a) une définition des informations à protéger (par exemple informations confidentielles);

b) la durée prévue de l'engagement, y compris les cas où cette durée n'est pas bornée;

c) les actions à engager lorsqu'un engagement arrive à expiration;

d) les responsabilités et les actions des signataires visant à éviter une diffusion d'informations non autorisée (telle que le «besoin d'en connaître»);

e) la propriété des informations, des secrets propres à l'activité de l'organisme et la propriété intellectuelle, ainsi que leurs liens avec la protection des informations confidentielles;

f) l'autorisation d'utiliser des informations confidentielles et les droits du signataire en matière d'utilisation de ces informations;

g) le droit, d'auditer et de contrôler des activités traitant des informations confidentielles;

h) le processus de notification et de remontée d'information dans le cadre d'une diffusion non autorisée ou de non-respect des exigences relatives à la confidentialité de l'information;

i) les modalités de retour ou de destruction d'informations à l'expiration de l'engagement;

j) les actions à engager en cas de violation de l'engagement.

Selon les exigences en matière de sécurité de l'organisme, il peut s'avérer nécessaire d'inclure d'autres dispositions dans les engagements de confidentialité ou de non-divulgation.

Il convient que les engagements de confidentialité et de non-divulgation soient conformes aux lois et règlements en vigueur dans la juridiction dont ils relèvent (voir également 15.1.1).

Il convient de réexaminer les engagements de confidentialité et de non-divulgation à intervalles réguliers et en cas de changements ayant un impact sur ces exigences.

Informations supplémentaires

Les engagements de confidentialité et de non-divulgation protègent les informations de l'organisme et informent les signataires de leur devoir de protéger, d'utiliser et de diffuser les informations de façon responsable et autorisée.

Selon les circonstances, un organisme peut avoir besoin de recourir à différentes formes d'engagements de confidentialité ou de non-divulgation.

6.1.6 Relations avec les autorités

Mesure

Il convient de mettre en place des relations appropriées avec les autorités compétentes.

Préconisations de mise en œuvre

Il convient que les organismes mettent en place des procédures spécifiant quand et comment les autorités compétentes (autorités chargées de l'application des lois, pompiers, autorités de surveillance) doivent être contactées. Les procédures définissent également comment les incidents liés à la sécurité de l'information doivent être signalés dans les meilleurs délais si une violation de la loi est suspectée.

Les organismes victimes d'attaques via Internet peuvent avoir besoin de faire appel à des tiers (par exemple à un fournisseur d'accès ou un opérateur de télécommunications) pour prendre des mesures contre la source des attaques.

Informations supplémentaires

La gestion de telles relations peut constituer une exigence destinée à appuyer la gestion des incidents (Paragraphe 13.2) ou le plan de continuité de l'activité et des mesures d'urgence (Article 14). Les contacts avec l'autorité légale sont également utiles pour anticiper et préparer les changements à venir au niveau législatif ou réglementaire devant être pris en compte par l'organisme. Les contacts avec d'autres autorités concernant les équipements, les services d'urgence, la santé et la sécurité, comme la brigade des pompiers (pour la continuité de l'activité), les opérateurs en télécommunication (pour le routage et la disponibilité) et les sociétés de distribution d'eau (pour le refroidissement du matériel).

6.1.7 Relations avec des groupes de spécialistes

Mesure

Il convient d'entretenir des contacts appropriés avec des groupes de spécialistes, des forums spécialisés dans la sécurité et des associations professionnelles.

Préconisations de mise en œuvre

Il convient d'envisager une inscription à des groupes d'intérêt ou des forums spécialisés aux fins suivantes

a) mieux connaître les meilleures pratiques et se tenir informé de l'évolution des connaissances relatives à la sécurité;

b) s'assurer que la connaissance de l'environnement de la sécurité de l'information est à jour et exhaustive;

c) recevoir à l'avance des alertes, des conseils et des correctifs logiciels concernant les attaques et les vulnérabilités;

d) avoir accès à des conseils de spécialistes sur la sécurité de l'information;

e) partager et échanger des informations sur les nouvelles technologies, les produits, les menaces ou les vulnérabilités;

f) mettre en place des relais d'information appropriés lors du traitement d'incidents liés à la sécurité de l'information (voir également 13.2.1).

Informations supplémentaires

Des accords de partage de l'information peuvent être établis en vue d'améliorer la coopération et la coordination dans le domaine de la sécurité. Il convient que de tels accords identifient les exigences en matière de protection des informations sensibles.

6.1.8 Revue indépendante de la sécurité de l'information

Mesure

Il convient de procéder à des revues régulières et indépendantes de l'approche retenue par l'organisme pour gérer et mettre en œuvre sa sécurité (à savoir le suivi des objectifs de sécurité, les politiques, les procédures et les processus relatifs à la sécurité de l'information); de telles revues sont également nécessaires lorsque des changements importants sont intervenus dans la mise en œuvre de la sécurité.

Préconisations de mise en œuvre

Il convient que les revues indépendantes soient réalisées à l'initiative de la direction. Des revues indépendantes sont nécessaires pour veiller à la pérennité de l'applicabilité, de l'adéquation et de l'efficacité de l'approche de l'organisme en matière de gestion de la sécurité de l'information. Il convient que la revue permette d'analyser les opportunités d'amélioration éventuelle et les changements à apporter en particulier à la politique et aux objectifs.

Il convient qu'une telle revue soit réalisée par des personnes indépendantes du domaine concerné, par exemple par des intervenants de la fonction d'audit interne, par un responsable indépendant ou un organisme tiers spécialisé dans de telles revues. Il convient que les personnes chargées de ces revues possèdent les compétences et l'expérience nécessaires.

Il convient d'enregistrer et de communiquer les résultats des revues à la direction à l'origine de la demande. Il convient de conserver ces enregistrements.

Si la revue indépendante met en lumière des inadéquations ou des non conformités dans l'approche ou la mise en œuvre de la sécurité de l'organisme par rapport aux directives énoncées dans la politique de sécurité de l'information (voir 5.1.1), il convient que la direction envisage des actions correctives.

Informations supplémentaires

La revue de la sécurité par domaine, régulièrement menée par les responsables concernés (voir 15.2.1), peut également être confiée à des personnes indépendantes. Les techniques de revues peuvent inclure des entretiens avec la direction, le contrôle des enregistrements ou le réexamen des politiques de sécurité. L'ISO 19011:2002, *Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental*, peut également fournir des directives utiles pour la réalisation de revues indépendantes, y compris pour l'établissement et la mise en œuvre de programmes de revues. En 15.3 sont pécifiées des mesures applicables à une revue indépendante portant sur un système d'information, ainsi que l'utilisation d'outils d'audit système.

6.2 Tiers

Objectif: assurer la sécurité de l'information et des moyens de traitement de l'information appartenant à l'organisme et consultés, opérés, communiqués ou gérés par des tiers.

Il convient que l'introduction de produits ou de services tiers ne nuise pas à la sécurité de l'information de l'organisme ni aux moyens de traitement de l'information.

Il convient de contrôler tout accès aux moyens de traitement de l'information ainsi que tout traitement et toute communication d'informations par des tiers.

Il convient de procéder à une appréciation du risque afin de déterminer les impacts sécurité et les mesures nécessaires lorsque l'organisme doit collaborer avec des tiers et leur autoriser l'accès aux informations ou aux moyens de traitement, ou lorsque l'organisme doit obtenir un produit et un service d'un tiers ou lui fournir un produit ou un service. Il convient que les parties concernées mettent en place des mesures et les définissent dans un agrément.

6.2.1 Identification des risques provenant des tiers

Mesure

Il convient d'identifier les risques pesant sur l'information et les moyens de traitement de l'organisme qui découlent d'activités impliquant des tiers, et de mettre en œuvre des mesures appropriées avant d'accorder des accès.

Préconisations de mise en œuvre

Lorsque est nécessaire d'accorder à un tiers un accès à l'information et aux moyens de traitement de l'information de l'organisme, il convient de procéder à une appréciation du risque (voir également Article 4) pour identifier les mesures complémentaires nécessaires. Il convient que l'identification des risques relatifs à l'accès par un tiers tienne compte des éléments suivants:

a) les moyens de traitement de l'information auxquels le tiers doit accéder;

b) le type d'accès qui sera accordé au tiers, à savoir:

   1) un accès physique, par exemple aux bureaux, aux salles d'ordinateurs et aux armoires de classement;

   2) un accès logique, par exemple aux bases de données et aux systèmes d'information de l'organisme;

   3) le type de connexion entre le réseau de l'organisme et celui du tiers, par exemple une connexion permanente ou un accès à distance;

   4) s'il s'agit d'un accès local ou distant;

c) la valeur et la sensibilité des informations concernées et leur criticité pour l'activité de l'organisme;

d) les mesures requises pour la protection de l'information qui n'est pas censée être accessible par le tiers;

e) le personnel externe concerné par le traitement de l'information;

f) le mode d'identification de l'organisme ou du personnel doté(e) des droits d'accès, le mode de vérification des droits et la fréquence à laquelle ces éléments doivent être confirmés;

g) les différents moyens et mesures mis en œuvre par le tiers lors du stockage, du traitement, de la communication, du partage et de l'échange d'informations;

h) l'impact d'une indisponibilité de l'accès par le tiers et l'incidence de la réception ou la saisie par le tiers d'informations erronées ou trompeuses;

i) les pratiques et procédures permettant de traiter les incidents liés à la sécurité de l'information et les dommages potentiels, ainsi que les dispositions relatives au maintien des accès en cas d'incident lié à la sécurité de l'information;

j) les exigences légales et réglementaires et les autres obligations contractuelles concernant le tiers et qu'il convient de prendre en compte;

k) l'incidence de ces dispositions sur toute autre partie prenante.

Il convient de ne pas accorder aux tiers de droits d'accès à l'information de l'organisme avant que des mesures appropriées aient été mises en œuvre et, le cas échéant, qu'un contrat ait été signé qui définisse les conditions de la connexion ou des droits d'accès, ainsi que les conditions de collaboration. En règle générale, il convient que l'ensemble des exigences en matière de sécurité résultant de la collaboration avec des parties externes ou de mesures internes soit retranscrit dans l'accord signé avec le tiers (voir également 6.2.2 et 6.2.3).

Il convient de s'assurer que le tiers est informé de ses obligations et accepte les responsabilités morales et financières qu'implique l'accès, le traitement, la communication ou la gestion de l'information et des moyens de traitement de l'information de l'organisme.

Informations supplémentaires

L'information peut être rendue vulnérable du fait d'une gestion inadaptée de la sécurité. Il convient d'identifier et d'appliquer des mesures pour gérer l'accès des tiers aux moyens de traitement de l'information. Par exemple, s'il existe un besoin particulier de confidentialité, il est possible de mettre en place des engagements de non-divulgation.

Les organismes peuvent faire face à des risques relatifs aux processus, à la gestion et à la communication entre plusieurs organismes en cas d'importants volumes de sous-traitance ou si plusieurs tiers sont impliqués.

Les mesures décrites en 6.2.2 et 6.2.3 présentent différents accords avec des tiers, à savoir:

a) les fournisseurs de service, tels que les FAI, les fournisseurs de service réseau, les services téléphoniques et les services de maintenance et d'assistance technique;

b) les services de gestion de la sécurité;

c) les clients;

d) les hébergeurs de moyens et/ou de services (systèmes informatiques, collecte de données centres d'appels);

e) les consultants et les auditeurs;

f) les développeurs et les fournisseurs, par exemple les éditeurs de logiciels et les fabricants de matériel informatique;

g) le nettoyage, la restauration et autres services d'assistance externalisés;

h) le personnel intérimaire, les contrats étudiants et autres affectations de courte durée.

De tels accords peuvent participer à la réduction des risques inhérents aux tiers.

6.2.2 La sécurité et les clients

Mesure

Tous les besoins de sécurité doivent être traités avant d'accorder aux clients l'accès à l'information ou aux biens de l'organisme.

Préconisations de mise en œuvre

Avant d'accorder aux clients l'accès aux biens de l'organisme, il convient d'examiner les éléments suivants (en fonction du type et de l'étendue des droits accordés, certains pouvant ne pas s'appliquer):

a) la protection des biens, y compris

   1) les procédures de protection des biens de l'organisme, y compris les informations et les logiciels, ainsi que la gestion des vulnérabilités connues,

   2) les procédures permettant de détecter une éventuelle compromission des biens, par exemple une perte ou une modification des données,

   3) l'intégrité, et

   4) les limites en matière de reproduction et de diffusion de l'information;

b) la description du produit ou du service à fournir;

c) les raisons, exigences et avantages divers justifiant l'accès des clients;

d) la politique de contrôle d'accès, qui couvre les aspects suivants:

   1) les méthodes d'accès autorisées ainsi que le contrôle et l'utilisation d'identifiants uniques, tels que les identifiants utilisateurs et les mots de passe;

   2) un processus d'autorisation pour l'accès et les privilèges des utilisateurs;

   3) une déclaration selon laquelle tout accès non autorisé de façon explicite est interdit;

   4) un processus de révocation des droits d'accès ou d'interruption de la connexion entre systèmes;

e) des dispositions relatives à la remontée, la notification et la recherche des informations inexactes (par exemple concernant les données personnelles), des incidents de sécurité et des failles de sécurité;

f) une description de chaque service rendu accessible;

g) le niveau de service cible et les niveaux de service inacceptables;

h) le droit de surveiller et de révoquer toute activité liée aux biens de l'organisme;

i) les responsabilités financières de l'organisme et du client;

j) les obligations légales et le mode de vérification du respect de ces obligations, par exemple la législation sur la protection des données, en tenant compte notamment des différents systèmes juridiques nationaux si l'accord prévoit une coopération internationale (voir également 15.1);

k) les droits de propriété intellectuelle et les droits de reproduction (voir 15.1.2) et la protection de tout travail collaboratif (voir également 6.1.5).

Informations supplémentaires

Les exigences en matière de sécurité s'appliquant aux clients ayant accès aux biens de l'organisme peuvent varier considérablement en fonction des moyens de traitement de l'information et des informations accédés. Ces exigences en matière de sécurité peuvent être traitées par le biais d'accords conclus avec le client traitant l'ensemble des risques et exigences identifiés en matière de sécurité (voir 6.2.1).

Les accords passés avec les clients peuvent également impliquer des tiers. Il convient que les accords autorisant un accès identifient d'autres parties éligibles et stipulent les conditions d'accès et le degré d'implication de ces dernières.

6.2.3 La sécurité dans les accords conclus avec des tiers

Mesure

Il convient que les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, couvrent l'ensemble des exigences applicables en matière de sécurité.

Préconisations de mise en œuvre

Il convient que l'accord garantisse l'absence de malentendu entre l'organisme et le tiers. Il convient que les organismes prévoient les dommages et intérêts du tiers.

Pour répondre aux exigences de sécurité (voir 6.2.1), il convient d'envisager d'inclure les conditions suivantes dans l'accord:

a) la politique de sécurité de l'information;

b) les mesures garantissant la protection des biens, à savoir:

   1) les procédures de protection des biens de l'organisme, y compris l'information, les logiciels et le matériel;

   2) toute mesure et mécanisme de protection physique requis;

   3) les mesures garantissant la protection contre des logiciels malveillants (voir 10.4.1);

   4) les procédures permettant de déterminer l'éventuelle compromission des biens, par exemple une perte ou une modification de l'information, du logiciel ou du matériel;

   5) les mesures garantissant le retour ou la destruction des informations et des biens à l'expiration de l'accord ou à tout autre moment fixé;

6) la confidentialité, l'intégrité, la disponibilité (voir 2.1.5) des biens et tout autre aspect pertinent;

7) les limites en matière de reproduction et de diffusion de l'information et l'utilisation d'accords de confidentialité (voir 6.1.5);

c) la formation des utilisateurs et des administrateurs aux méthodes, aux procédures et à la sécurité;

d) la sensibilisation des utilisateurs en matière de sécurité et de responsabilité;

e) les dispositions concernant le transfert du personnel, le cas échéant;

f) les responsabilités en matière d'installation et de maintenance logicielle et matérielle;

g) une structure de remontée de l'information claire et des formats approuvés;

h) un processus clair et défini relatif à la gestion des modifications;

i) la politique de contrôle d'accès, qui couvre les points suivants:

1) les raisons, exigences et avantages divers de l'attribution de droits d'accès aux tiers;

2) les méthodes d'accès autorisées ainsi que le contrôle et l'utilisation d'identifiants uniques, tels que les identifiants et les mots de passe utilisateurs;

3) un processus d'autorisation pour l'accès et les privilèges des utilisateurs;

4) la nécessité de gérer une liste des personnes habilitées à utiliser les services rendus accessibles et une description de leurs droits et privilèges;

5) une déclaration selon laquelle tout accès non autorisé de façon explicite est interdit;

6) un processus de révocation des droits d'accès ou d'interruption de la connexion entre systèmes;

j) des dispositions relatives à la remontée, la notification et la recherche des incidents et des failles de sécurité, ainsi que sur le non-respect des exigences énoncées dans l'accord;

k) une description du produit ou du service à fournir ainsi qu'une description de l'information à mettre à disposition, accompagnée d'une classification de sa sécurité (voir 7.2.1);

l) le niveau de service cible et les niveaux de service inacceptables;

m) la définition de critères de performances vérifiables, leur suivi et leur signalement;

n) le droit de surveiller et révoquer toute activité liée aux biens de l'organisme;

o) le droit d'auditer les responsabilités définies dans l'accord, d'attribuer la réalisation de ces audits à des tiers et de définir les droits des auditeurs;

p) la définition d'une procédure progressive de résolution de problèmes;

q) les exigences de continuité de service, y compris les mesures de disponibilité et de fiabilité, conformément aux priorités de l'organisme;

r) les responsabilités financières des parties;

s) les obligations légales et le mode de vérification du respect des exigences, par exemple la législation sur la protection des données, notamment en tenant compte des différents systèmes juridiques nationaux si l'accord prévoit une coopération internationale (voir également 15.1);

t) les droits de propriété intellectuelle et les droits de reproduction (voir 15.1.2), ainsi que la protection de tout travail collaboratif (voir également 6.1.5);

u) l'implication du tiers vis-à-vis de ses sous-traitants et les mesures de sécurité que les contractants doivent mettre en œuvre;

v) les conditions de renégociation/résiliation des accords:

   1) il convient d'élaborer un plan de secours dans le cas où l'une des parties souhaiterait mettre fin aux relations avant l'expiration des accords;

   2) la renégociation des accords si les exigences de sécurité de l'organisme changent;

   3) la documentation des listes de biens, licences, accords ou droits y afférant.

Informations supplémentaires

Les accords peuvent considérablement différer d'un organisme à l'autre et selon les tiers. Par conséquent, il convient de veiller à inclure l'ensemble des risques identifiés et des exigences en matière de sécurité (voir également 6.2.1) dans les accords. Le cas échéant, les procédures et mesures requises peuvent être développées dans un plan de gestion de la sécurité.

Si la gestion de la sécurité de l'information est externalisée, il convient que les accords définissent la manière dont le tiers va garantir le niveau de sécurité adéquat, conformément à l'appréciation du risque, et comment il va adapter la sécurité en vue de prendre en compte l'évolution des risques.

Certaines différences entre l'externalisation et les autres formes de services assurés par les tiers portent sur la question de la responsabilité financière, la planification de la période transitoire et l'interruption potentielle de l'activité sur la période, les accords quant aux plan de secours et aux revues d'urgence ainsi que sur la collecte et la gestion d'informations sur les incidents liés à la sécurité. Par conséquent, il est important que l'organisme planifie et gère la transition vers des moyens externalisés et qu'il établisse des processus adaptés en vue de gérer les changements et la renégociation/résiliation des accords.

Il est nécessaire de stipuler dans l'accord les procédures de continuité de l'activité dans le cas où le tiers cesserait de fournir ses services, afin d'éviter tout retard dans la mise en place de services de remplacement.

Les accords passés avec les clients peuvent également impliquer des tiers. Il convient que les accords autorisant un accès identifient d'autres parties éligibles et stipulent les conditions d'accès et le degré d'implication de ces dernières.

En règle générale, les accords sont d'abord mis au point par l'organisme. Dans certaines circonstances, un tiers peut élaborer et imposer un accord à un organisme. L'organisme doit alors s'assurer que sa propre politique de sécurité n'est pas inutilement mise en cause par les exigences stipulées dans des accords imposés par le tiers.

7 Gestion des biens

7.1 Responsabilités relatives aux biens

Objectif: mettre en place et maintenir une protection appropriée des biens de l'organisme.

Il convient d'inventorier tous les biens et de leur attribuer un propriétaire.

Il convient d'identifier des propriétaires pour tous les biens et d'attribuer la responsabilité de la gestion des mesures appropriées. La mise en œuvre de mesures spécifiques peut être déléguée par le propriétaire, mais ce dernier demeure responsable de la protection des biens.

7.1.1 Inventaire des biens

Mesure

Il convient de clairement identifier tous les biens, de réaliser et de gérer un inventaire de tous les biens importants.

Préconisations de mise en œuvre

Il convient qu'un organisme identifie tous les biens et documente l'importance de ces derniers. Il convient que l'inventaire des biens comporte toutes les informations nécessaires pour faire face à un sinistre, en particulier le type de bien, son format, son emplacement, les informations relatives à sa sauvegarde et à la licence, ainsi que sa valeur pour l'organisme. Il convient de ne pas dupliquer inutilement d'autres inventaires, mais il convient de garantir un alignement du contenu.

En outre, il convient de parvenir à un accord sur la propriété des biens (voir 7.1.2) et la classification des informations (voir 7.2) et de répertorier ces éléments dans un document. En fonction de l'importance du bien, de sa valeur pour l'organisme et de sa classification, il convient de définir des niveaux de protection proportionnels à l'importance des biens (pour plus ample information sur le mode d'évaluation des biens, voir l'ISO/CEI TR 13335-3).

Informations supplémentaires

Il existe plusieurs types de biens, qui comprennent les éléments suivants:

a) l'information: les bases de données et les fichiers de données, les contrats et les accords, la documentation système, les informations de recherche, les manuels utilisateur, le matériel de formation, les procédures opérationnelles ou de support, le plan de continuité de l'activité, les accords de repli, les traces d'audit et les informations archivées;

b) les biens logiciels: les applications logicielles les logiciels système, les outils de développement et les utilitaires;

c) les biens physiques: le matériel informatique, les moyens de communication, les supports amovibles et autre matériel;

d) les services: les services informatiques et de télécommunication, ainsi que les moyens connexes, tels que le chauffage, l'éclairage, l'alimentation électrique et la climatisation;

e) les personnes et leurs qualifications, leur savoir-faire et leur expérience;

f) les valeurs immatérielles, comme la réputation et l'image de l'organisme.

L'inventaire des biens permet de mettre en place une protection des biens efficace et peut également s'avérer nécessaire à d'autres fins pour l'organisme, par exemple dans le cadre de la santé et de la sécurité des personnes, des polices d'assurance ou pour des raisons financières (gestion des biens). Le processus de réalisation d'un inventaire des biens constitue une condition requise importante dans le management du risque (voir également Article 4).

7.1.2 Propriété des biens

Mesure

Il convient d'attribuer la propriété[2)] de chaque information et moyens de traitement de l'information à une partie définie de l'organisme.

Préconisations de mise en œuvre

Il convient que le propriétaire des biens soit responsable

a) de la classification correcte des informations et des biens associés aux moyens de traitement de l'information, et

b) de la définition et du réexamen périodique des limites et des classifications d'accès, en tenant compte des politiques de contrôle d'accès applicables.

La propriété peut être affectée

a) à un processus métier,

b) à un ensemble défini d'activités,

c) à une application, ou

d) à un ensemble défini de données.

Informations supplémentaires

Les tâches de routine peuvent être déléguées, par exemple à un dépositaire veillant quotidiennement sur le bien, mais la responsabilité du bien demeure attachée au propriétaire.

Dans le cas de systèmes d'information complexes, il peut s'avérer utile de désigner des groupes de biens ayant une fonction de «services» particulière. Le responsable du service est alors responsable de la prestation du service, y compris du fonctionnement des biens assurant ce service.

7.1.3 Utilisation correcte des biens

Mesure

Il convient d'identifier, de documenter et de mettre en œuvre des règles permettant l'utilisation correcte de l'information et des biens associés aux moyens de traitement de l'information.

Préconisations de mise en œuvre

Il convient que tous les salariés, contractants et utilisateurs tiers suivent les règles relatives à l'utilisation correcte de l'information et des biens associés aux moyens de traitement de l'information, à savoir:

a) les règles d'utilisation des messageries électroniques et d'Internet (voir 10.8);

b) les lignes directrices relatives à l'utilisation d'appareils mobiles, notamment à leur utilisation hors des locaux de l'organisme (voir 11.7.1);

---

2) Le terme «propriétaire» identifie une personne ou une entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des biens. Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur le bien.

Il convient que les règles spécifiques ou les lignes directrices soient fournies par le responsable concerné. Il convient que les salariés, contractants et utilisateurs tiers employant ou ayant accès aux biens de l'organisme soient conscients des limites de l'utilisation de l'information et des biens de l'organisme associés aux moyens de traitement de l'information et aux ressources. Il convient qu'ils soient responsables de l'utilisation de toute ressource de traitement de l'information et de toute utilisation effectuée sous leur responsabilité.

7.2 Classification des informations

Objectif: garantir un niveau de protection approprié aux informations.

Il convient de classifier les informations pour indiquer le besoin, les priorités et le degré souhaité de protection lors de leur manipulation.

Les informations peuvent présenter des degrés divers de sensibilité et de criticité. Certaines informations peuvent nécessiter un niveau de protection spécial ou une manipulation particulière. Il convient d'élaborer un plan de classification des informations pour hiérarchiser les niveaux de protection et informer les personnes intéressées des besoins de manipulations particulières.

7.2.1 Lignes directrices pour la classification

Mesure

Il convient de classer les informations en termes de valeur, d'exigences légales, de sensibilité et de criticité.

Préconisations de mise en œuvre

Il convient que les classifications et les mesures de protection associées tiennent compte des besoins fonctionnels en matière de partage ou de limitation des informations, ainsi que des impacts sur l'activité de l'organisme.

Il convient que les lignes directrices de classification prévoient une classification initiale et un réexamen de cette classification au fil du temps, de manière cohérente avec la politique de contrôle d'accès prédéfinie (voir 11.1.1).

Il convient que le propriétaire du bien soit responsable (voir 7.1.2) de la classification du bien, du réexamen et de la mise à jour de cette classification. Il convient que la classification tienne compte de l'effet d'agrégation mentionné en 10.7.2.

Il convient de tenir compte des différents niveaux possibles de classification et de leurs avantages Les schémas excessivement complexes peuvent s'avérer fastidieux et peu rentables, voire irréalisables. Il convient d'interpréter avec soin les marques de classification des documents provenant d'autres organismes: les mêmes marques peuvent renvoyer à des niveaux de sensibilité différents.

Informations supplémentaires

Le niveau de sensibilité peut être apprécié en analysant la confidentialité, l'intégrité, la disponibilité et toute autre exigence relatives aux informations à évaluer.

Les informations cessent souvent d'être sensibles ou critiques après une période donnée, par exemple une fois que les informations ont été rendues publiques. Il convient de prendre ces aspects en compte, car une sur classification peut entraîner la mise en œuvre de mesures inutiles et in fine des dépenses supplémentaires.

Procéder par analogie avec des documents présentant des besoins similaires peut faciliter le travail de classification.

En règle générale, la classification des informations conditionne le mode de traitement et de protection de ces informations.

7.2.2 Marquage et manipulation de l'information

Mesure

Il convient d'élaborer et de mettre en œuvre un ensemble approprié de procédures pour le marquage et la manipulation de l'information, conformément au plan de classification adopté par l'organisme.

Préconisations de mise en œuvre

Les procédures de marquage de l'information doivent être applicables à des actifs aux formats physique et électronique.

Il convient que les données délivrées par des systèmes contenant des informations classifiées comme sensibles ou critiques portent des étiquettes appropriées. Il convient que le marquage reflète la classification, telle que définie en 7.2.1. Les éléments à prendre en compte comprennent les rapports écrits, les données affichées à l'écran, les données enregistrées (par exemple sur cassettes, disques ou CD), les messages électroniques et les transferts de fichiers.

Pour chaque niveau de classification, il convient de définir des procédures, telles que le traitement sécurisé, le stockage, la transmission, la déclassification et la destruction. Il convient également de prévoir des procédures pour la garde et la journalisation de tout événement lié à la sécurité.

Il convient que les accords conclus avec d'autres organismes traitant des informations partagées prévoient des procédures permettant d'identifier la classification des informations et d'interpréter les marques de classification émises ou délivrées.

Informations supplémentaires

Le marquage et le traitement sécurisé des informations classifiées constituent une exigence clé dans les accords de partage d'informations. Le marquage matériel constitue une forme de marquage courante. Cependant, certains actifs immatériels, tels des documents sous forme électronique, ne peuvent pas être physiquement étiquetés et des moyens électroniques sont nécessaires. Par exemple, une marque d'avertissement peut apparaître à l'écran. Lorsque le marquage s'avère irréalisable, il est possible de recourir à d'autres moyens pour signifier la classification des informations, par exemple à l'aide de procédures ou de métadonnées.

8 Sécurité liée aux ressources humaines

8.1 Avant le recrutement

Objectif: garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils conviennent pour les fonctions qui leur sont attribuées et réduire le risque de vol, de fraude ou de mauvais usage des équipements.

Il convient de mentionner les responsabilités en matière de sécurité avant l'embauche, dans des descriptions de poste adéquates, puis dans le contrat de travail.

Il convient de sélectionner avec soin tous les postulants, contractants et utilisateurs tiers, surtout lorsqu'il s'agit de tâches sensibles.

Il convient que les salariés, contractants et utilisateurs tiers de moyens de traitement de l'information signent un accord sur leurs rôles et responsabilités en matière de sécurité.

8.1.1 Rôles et responsabilités

Mesure

Il convient de définir et de documenter les rôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs tiers, conformément à la politique de sécurité de l'information de l'organisme.

Préconisations de mise en œuvre

Il convient que les rôles et responsabilités en matière de sécurité précisent les exigences relatives aux points suivants:

a) mise en œuvre et d'application conformément aux politiques de sécurité de l'information de l'organisme (voir 5.1);

b) protection des biens contre un accès, une diffusion, une modification, une destruction ou une intrusion non autorisés;

c) exécution d'activités ou de processus de sécurité particuliers;

d) affectation de responsabilité à la personne ayant commis des actes;

e) signalement d'événements de sécurité, d'événements potentiels ou d'autres risques liés à la sécurité de l'organisme.

Il convient d'informer clairement le candidat des rôles et responsabilités en matière de sécurité au cours du processus de préembauche.

Informations supplémentaires

Les descriptions de postes peuvent servir à documenter les rôles et responsabilités en matière de sécurité. Il convient que les rôles et les responsabilités attribués aux personnes engagées via un organisme tiers, soient clairement définis et indiqués.

8.1.2 Sélection

Mesure

Qu'il s'agisse de postulants, de contractants ou d'utilisateurs tiers, il convient que les vérifications des informations concernant tous les candidats soient réalisées conformément aux lois, aux règlements et à l'étique et qu'elles soient proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

Préconisations de mise en œuvre

Il convient que les vérifications prennent en compte le droit du travail et la législation relative à la protection de la vie privée et/ou les données personnelles, et que les vérifications comportent, lorsque cela s'avère possible, les aspects suivants:

a) des références satisfaisantes sur les qualités personnelles, par exemple sur les plans professionnel et personnel;

b) un contrôle (de l'état complet et de la précision) du curriculum vitæ du candidat;

c) la confirmation des formations et des qualifications professionnelles alléguées;

d) un contrôle d'identité indépendant (passeport ou document similaire);

e) des contrôles plus détaillés, par exemple sur la solvabilité ou sur le casier judiciaire.

Qu'il s'agisse d'une première embauche ou d'une promotion, lorsqu'un poste nécessite l'accès aux moyens de traitement de l'information et en particulier s'il s'agit d'informations sensibles, par exemple financières ou hautement confidentielles, il convient que l'organisme envisage des contrôles plus détaillés.

Il convient que les procédures définissent des critères et des limites pour les vérifications, par exemple qui est habilité à réaliser une telle enquête, de quelle manière, à quel moment et pour quelles raisons.

Il convient également de sélectionner sur dossier les contractants et les utilisateurs tiers. Lorsque les contractants sont sélectionnés par une agence, il convient que le contrat passé avec cette dernière spécifie de manière claire les responsabilités de l'agence en matière de sélection sur dossier, ainsi que les procédures de notification à suivre si la sélection sur dossier n'a pas été intégralement réalisée ou si les résultats s'avèrent inquiétants ou sèment le doute. De même, il convient que l'accord avec le tiers (voir également 6.2.3) spécifie clairement toutes les responsabilités et procédures de notification relatives à la sélection.

Il convient de rassembler les informations sur tous les candidats envisagés pour des embauches au sein de l'organisme et de les traiter conformément à toute législation en vigueur dans la juridiction dont ils relèvent. Selon la législation en vigueur, il convient ou non que les candidats soient informés de la procédure de sélection sur dossier avant qu'elle soit lancée.

8.1.3 Conditions d'embauche

Mesure

Dans le cadre de leurs obligations contractuelles, il convient que les salariés, contractants et utilisateurs tiers se mettent d'accord sur les modalités du contrat d'embauche les liant et le signent. Il convient que ce contrat définisse les responsabilités de l'organisme et de l'autre partie quant à la sécurité de l'information.

Préconisations de mise en œuvre

Il convient que les conditions d'embauche reflètent la politique de sécurité de l'organisme et stipulent clairement les aspects suivants:

a) il convient que tous les salariés, contractants et utilisateurs tiers ayant accès à l'information sensible signent un engagement de confidentialité ou de non-divulgation avant d'obtenir l'accès aux moyens de traitement de l'information;

b) les responsabilités juridiques et les droits des salariés, contractants et d'utilisateurs tiers concernant par exemple les droits de reproduction et la législation sur la protection des données (voir également 15.1.1 et 15.1.2);

c) les responsabilités relatives à la classification des informations et à la gestion des biens de l'organisme associés aux systèmes d'information et aux services que le salarié, le contractant ou l'utilisateur tiers utilise (voir également 7.2.1 et 10.7.3);

d) les responsabilités du salarié, du contractant ou de l'utilisateur tiers quant à la manipulation de l'information reçue d'autres organismes ou de tiers;

e) les responsabilités de l'organisme relatives à la manipulation des données personnelles, y compris les données créées au cours ou à la suite de la période de travail au sein de l'organisme (voir également 15.1.4);

f) les responsabilités qui s'appliquent hors des locaux de l'organisme et des heures de travail normales, notamment dans le cadre du télétravail (voir également 9.2.5 et 11.7.1);

g) les actions à engager si le salarié, le contractant ou l'utilisateur tiers ne tient pas compte des exigences en matière de sécurité de l'organisme (voir également 8.2.3).

Il convient que l'organisme s'assure que les salariés, contractants et utilisateurs tiers approuvent les dispositions relatives à la sécurité de l'information concernant la nature et l'étendue de leur futur accès aux biens de l'organisme associés aux systèmes d'information et aux services.

Le cas échéant, il convient que les responsabilités stipulées dans le contrat de travail continuent à s'appliquer pendant une durée définie après la fin du contrat (voir également 8.3).

Informations supplémentaires

Il est possible de recourir à un code de conduite pour définir les responsabilités du salarié, du contractant et de l'utilisateur tiers quant à la confidentialité, la protection des données, l'éthique, l'utilisation appropriée de l'équipement et du matériel de l'organisme, ainsi qu'aux bonnes pratiques attendues par l'organisme. Le contractant ou les utilisateurs tiers peuvent être associés à un organisme externe pouvant être amené lui aussi à conclure des accords contractuels au nom de la personne liée par le contrat.

8.2 Pendant la durée du contrat

Objectif: veiller à ce que salariés, contractants et utilisateurs tiers soient conscients des menaces pesant sur la sécurité de l'information, de leurs responsabilités financières ou autres, et de la nécessité de disposer des éléments requis pour prendre en charge la politique de sécurité de l'organisme dans le cadre de leur activité normale et de réduire le risque d'erreur humaine.

Il convient de définir les responsabilités de la direction qui doit s'assurer de l'application de la sécurité confiée par contrat à une personne au sein de l'organisme.

Il convient de permettre à l'ensemble des salariés, contractants et utilisateurs tiers de bénéficier d'un niveau adéquat de qualification, formation et sensibilisation aux procédures de sécurité et à l'utilisation correcte des moyens de traitement de l'information, en vue de réduire le plus possible le risque lié à la sécurité. Il convient d'élaborer un processus disciplinaire formel pour les salariés ayant enfreint les règles de sécurité.

8.2.1 Responsabilités de la direction

Mesure

Il convient que la direction demande aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme.

Préconisations de mise en œuvre

Il relève des responsabilités de la direction que les salariés, contractants et utilisateurs tiers:

a) soient correctement informés sur leurs fonctions et responsabilités en matière de sécurité de l'information avant d'avoir accès à l'information sensible ou aux systèmes d'information;

b) prennent connaissance des lignes directrices concernant les attentes en matière de sécurité dans le cadre de leurs fonctions au sein de l'organisme;

c) soient incités à appliquer les politiques de sécurité de l'organisme;

d) acquièrent un niveau de sensibilisation à la sécurité en adéquation avec leurs fonctions et responsabilités au sein de l'organisme (voir également 8.2.2);

e) respectent les conditions d'embauche, y compris la politique de sécurité de l'information de l'organisme et sur les méthodes de travail appropriées;

f) maintiennent leur savoir-faire et leurs qualifications à niveau.

Informations supplémentaires

Si rien n'est entrepris pour sensibiliser les salariés, contractants et utilisateurs tiers quant à leurs responsabilités en matière de sécurité, ces derniers peuvent causer des préjudices considérables à un organisme. Le personnel motivé est susceptible d'être plus fiable et à l'origine d'une moindre quantité d'incidents liés à la sécurité de l'information.

Une direction n'apportant pas satisfaction peut donner au personnel le sentiment d'être peu estimé, ce qui peut avoir un impact négatif sur la sécurité de l'organisme. Par exemple, une telle direction peut entraîner une certaine négligence en matière de sécurité ou un mauvais usage des biens de l'organisme.

8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information

Mesure

Il convient que l'ensemble des salariés d'un organisme et, le cas échant, les contractants et utilisateurs tiers suivent une formation adaptée sur la sensibilisation et reçoivent régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions.

Préconisations de mise en œuvre

Il convient qu'une formation sur la sensibilisation commence par une période d'intégration formelle destinée à présenter les politiques de sécurité et les attentes de l'organisme, avant que l'accès à l'information ou aux services soit donné.

Il convient qu'une formation continue traite des exigences en matière de sécurité, des responsabilités juridiques et des mesures d'exploitation, ainsi que de l'utilisation correcte des moyens de traitement de l'information, par exemple la procédure de connexion, l'utilisation de progiciels et les informations sur le processus disciplinaire (voir 8.2.3).

Informations supplémentaires

Il convient que les activités relatives à la sensibilisation, la qualification et aux formations en matière de sécurité soient adaptées à la fonction, aux responsabilités et au savoir-faire de la personne et qu'elles comprennent des informations sur les menaces connues, sur les personnes à contacter pour obtenir davantage de conseils en matière de sécurité et sur les canaux à utiliser pour signaler les incidents liés à la sécurité de l'information (voir également 13.1).

La formation destinée à accroître la sensibilisation a pour finalité de permettre aux personnes de reconnaître des problèmes et des incidents liés à la sécurité de l'information et de répondre en fonction des besoins de leur fonction.

8.2.3 Processus disciplinaire

Mesure

Il convient d'élaborer un processus disciplinaire formel pour les salariés ayant enfreint les règles de sécurité.

Préconisations de mise en œuvre

Il convient que le processus disciplinaire ne débute pas avant qu'une première vérification de la brèche dans la sécurité ait été effectuée (voir également 13.2.3 à propos de la collecte de preuves).

Il convient que le processus disciplinaire formel garantisse un traitement correct et juste des salariés suspectés d'avoir enfreint les règles de sécurité. Il convient que le processus disciplinaire formel fournisse une réponse graduée prenant en considération des facteurs tels que la nature et la gravité de la violation, ainsi que son impact sur l'activité de l'organisme. Il convient également de préciser s'il s'agit d'une première infraction ou d'une récidive, si le contrevenant a reçu la formation adéquate, et de considérer les dispositions légales applicables, les contrats commerciaux et tout autre facteur nécessaire. En cas de mauvaise conduite flagrante, il convient que le processus prévoie le retrait immédiat des fonctions, des droits d'accès et des privilèges, et une mise à pied immédiate, le cas échéant.

Informations supplémentaires

Il convient également que le processus disciplinaire constitue un élément dissuasif empêchant les salariés, contractants et utilisateurs tiers d'enfreindre les politiques et procédures relatives à la sécurité de l'organisme et toute autre règle de sécurité.

8.3 Fin ou modification de contrat

Objectif: veiller à ce que les salariés, contractants et utilisateurs tiers quittent un organisme ou changent de poste selon une procédure définie.

Il convient que les responsabilités existent pour garantir la bonne gestion du départ d'un salarié, contractant ou utilisateur tiers, et que la restitution de tout le matériel et la suppression de tous les droits d'accès soient effectuées.

Il convient qu'une modification des responsabilités et des fonctions au sein d'un organisme soit gérée comme une fin de contrat, telle que décrite à l'Article 8, et que toute nouvelle prise de fonctions soit gérée telle que décrite en 8.1.

8.3.1 Responsabilités en fin de contrat

Mesure

Il convient que les responsabilités relatives aux fins ou aux modifications de contrats soient clairement définies et attribuées.

Préconisations de mise en œuvre

Il convient que les responsabilités relatives aux fins de contrats incluent les exigences en matière de sécurité permanente et les responsabilités juridiques et, le cas échéant, les responsabilités contenues dans tout engagement de confidentialité (voir 6.1.5) et les conditions d'embauche (voir 8.1.3) se poursuivant pendant une période définie au-delà de la fin de l'emploi du salarié, du contractant ou de l'utilisateur tiers.

Il convient que les responsabilités et attributions de tâches encore valables après la fin du contrat figurent dans le contrat du salarié, du contractant ou de l'utilisateur tiers.

Il convient de gérer les modifications de responsabilités comme une fin de contrat et de traiter les nouvelles responsabilités ou fonctions comme décrit en 8.1.

Informations supplémentaires

Le service des ressources humaines est généralement responsable de la totalité du processus de résiliation et travaille de pair avec le supérieur du salarié concerné en vue de gérer les aspects relatifs à la sécurité des procédures. Dans le cas d'un contractant, les responsabilités en matière de résiliation du contrat peuvent être endossées par une agence traitant le dossier du contractant et, dans le cas d'un utilisateur tiers, l'organisme de ce dernier peut se charger de la résiliation.

Il peut s'avérer nécessaire d'informer les salariés, clients, contractants ou utilisateurs tiers des changements apportés aux dispositions relatives aux effectifs et à l'exploitation.

8.3.2 Restitution des biens

Mesure

Il convient que tous les salariés, contractants et utilisateurs tiers restituent la totalité des biens de l'organisme qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord.

Préconisations de mise en œuvre

Il convient que le processus de résiliation soit formalisé et qu'il prévoie la restitution de l'ensemble des logiciels, des documents et du matériel appartenant à l'organisme. Les autres biens appartenant à l'organisme, tels que les appareils d'informatique mobile, les cartes de crédit, les cartes d'accès, les logiciels, les manuels et les informations stockées sur des supports électroniques, doivent également être restitués.

Si un salarié, un contractant ou un utilisateur tiers achète du matériel à l'organisme ou utilise son propre matériel, il convient de suivre des procédures pour garantir que toutes les informations pertinentes soient transférées à l'organisme et correctement effacées du matériel (voir également 10.7.1).

Si un salarié, un contractant ou un utilisateur tiers détient des connaissances importantes au sujet des activités en cours, il convient que ces informations soient documentées et transférées à l'organisme.

8.3.3 Retrait des droits d'accès

Mesure

Il convient que les droits d'accès de l'ensemble des salariés, contractants et utilisateurs tiers à l'information et aux moyens de traitement de l'information soient supprimés à la fin de leur période d'emploi, ou modifiés en cas de modification du contrat ou de l'accord.

Préconisations de mise en œuvre

À la fin du contrat, il convient de reconsidérer les droits d'accès d'une personne aux biens liés aux systèmes d'information et aux services, afin de déterminer s'il est nécessaire de supprimer ces droits. Il convient que les modifications apportées à un contrat entraînent le retrait de tous les droits d'accès n'ayant pas été approuvés dans le cadre du nouveau contrat. Il convient que les droits d'accès à supprimer ou à adapter concernent les accès physiques et logiques, les clés, les cartes d'identification, les moyens de traitement de l'information (voir également 11.2.4), les abonnements et la suppression de toute documentation identifiant le salarié comme un membre de l'organisme. Si un salarié, un contractant ou un utilisateur tiers quittant l'organisme connaît les mots de passe de comptes restés actifs, il convient de changer ces mots de passe lors de la résiliation ou de la modification du contrat ou de l'accord.

Il convient que les droits d'accès aux actifs informationnels et aux moyens de traitement de l'information soient réduits ou supprimés avant la fin ou la modification du contrat en fonction de l'évaluation des facteurs de risque, tels que les suivants:

a) s'agit-il d'une résiliation ou d'une modification du contrat à l'initiative du salarié, du contractant ou de l'utilisateur tiers ou de la direction et pour quel motif ?

b) quelles sont les responsabilités du salarié, du contractant ou de tout autre utilisateur ?

c) quelle est la valeur des biens accessibles ?

Informations supplémentaires

Dans certaines circonstances, les droits d'accès peuvent être attribués afin de les rendre utilisables par davantage de personnes que le seul salarié, contractant ou utilisateur tiers quittant l'organisme, par exemple par des identifiants de groupe. Dans ce cas, il convient de supprimer les noms des personnes quittant l'organisme de toute liste d'accès de groupe et de prendre les dispositions nécessaires pour demander à l'ensemble des autres salariés, contractants et utilisateurs tiers de cesser de partager des informations avec la personne quittant l'organisme.

Lorsque la direction est à l'origine de la résiliation du contrat, les salariés, contractants ou utilisateurs tiers mécontents peuvent chercher délibérément à altérer les données ou à saboter les moyens de traitement de l'information. S'il s'agit de départs volontaires, les personnes peuvent être tentées de recueillir des informations en vue d'une utilisation ultérieure.

9 Sécurité physique et environnementale

9.1 Zones sécurisées

Objectif: empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux et les informations de l'organisme.

Il convient que les moyens de traitement des informations sensibles ou critiques soient abrités dans des zones sécurisées, protégés par des périmètres de sécurité définis, présentant des barrières de sécurité et des contrôles à l'entrée appropriés. Il convient que ces équipements soient protégés physiquement contre les accès non autorisés, les dommages et les intrusions.

Il convient d'adapter la protection en fonction des risques identifiés.

9.1.1 Périmètre de sécurité physique

Mesure

Il convient de protéger les zones contenant des informations et des moyens de traitement de l'information par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil).

Préconisations de mise en œuvre

Le cas échéant, il convient d'envisager et de mettre en œuvre les directives suivantes sur les périmètres de sécurité physique:

a) il convient de définir clairement les périmètres de sécurité et de décider de l'emplacement et du niveau de résistance de chacun des périmètres selon les exigences relatives à la sécurité des biens situés à l'intérieur et les conclusions de l'appréciation du risque;

b) il convient que les périmètres d'un bâtiment ou d'un site abritant des moyens de traitement de l'information soient physiquement solides (il convient que le périmètre ou les zones ne présente aucune faille susceptible de permettre facilement une intrusion); il convient que les murs extérieurs du site soient construits dans des matériaux robustes et que toutes les portes extérieures soient adéquatement protégées contre les accès non autorisés par des mécanismes de contrôle, par exemple des barres, des alarmes, des verrous; il convient également de verrouiller les portes et fenêtres non surveillées et d'envisager une protection extérieure pour les fenêtres, particulièrement celles du rez-de-chaussée;

c) il convient de placer du personnel à l'accueil ou d'autres moyens de contrôle d'accès physique au site ou au bâtiment; il convient de limiter l'accès aux sites et aux bâtiments aux seules personnes habilitées.

d) s'il y a lieu, il convient d'ériger des barrières physiques pour empêcher l'accès physique non autorisé et la contamination de l'environnement;

e) conjointement aux murs, il convient d'équiper d'une alarme l'ensemble des portes coupe-feu du périmètre de sécurité, de surveiller ces portes et de les soumettre à essai régulièrement, pour atteindre le niveau de résistance requis conformément aux normes régionales, nationales et internationales; il convient qu'elles fonctionnent conformément au code incendie local et qu'elles soient dotées d'une sécurité intégrée.

f) il convient d'installer des systèmes de détection d'intrus adaptés, conformes aux normes nationales, régionales et internationales et de les soumettre à essai régulièrement pour couvrir l'ensemble des portes extérieures et des fenêtres accessibles; il convient que les alarmes des zones inoccupées soient activées en permanence; il convient également de couvrir les autres zones, comme la salle des ordinateurs ou la salle des télécommunications;

g) il convient de séparer physiquement les moyens de traitement de l'information gérés par l'organisme et ceux gérés par des tiers.

Informations supplémentaires

La protection physique peut être assurée en créant une ou plusieurs barrières physiques autour des locaux et des moyens de traitement de l'information de l'organisme. L'utilisation de barrières multiples offrant un surcroît de protection, la défaillance d'une seule barrière ne compromet pas immédiatement la sécurité.

La zone sécurisée peut être un bureau fermé à clé ou plusieurs salles ceintes d'une barrière de sécurité physique continue. Des barrières et des périmètres supplémentaires de contrôle d'accès physique peuvent être nécessaires entre des zones soumises à des exigences de sécurité différentes à l'intérieur d'un même périmètre de sécurité.

Il convient de prendre spécialement en compte la sécurité de l'accès physique aux bâtiments multi-occupants.

9.1.2 Contrôles physiques des accès

Mesure

Il convient de protéger les zones sécurisées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité soit admis.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes:

a) il convient de consigner la date et l'heure d'arrivée et de départ des visiteurs et il convient que tous les visiteurs soient accompagnés sauf si leur accès a déjà été autorisé; il convient de leur accorder l'accès uniquement à des fins précises ayant fait l'objet d'une autorisation et de leur remettre les instructions relatives aux exigences de sécurité de la zone et aux procédures d'urgence associées;

b) concernant les zones dans lesquelles des informations sensibles sont traitées ou stockées, il convient de contrôler l'accès et de le limiter aux seules personnes habilitées. Il convient de prévoir des contrôles d'authentification, comme les cartes d'accès accompagnées d'un numéro d'identification personnelle pour autoriser et valider tous les accès. Il convient de tenir à jour de façon sécurisée une trace d'audit de tous les accès;

c) il convient d'exiger de l'ensemble des salariés, contractants et utilisateurs tiers et de tous les visiteurs le port d'un moyen identification visible. Il convient qu'ils informent immédiatement le personnel de sécurité s'ils rencontrent des visiteurs non accompagnés ou quiconque ne portant pas d'identification visible;

d) concernant les zones sécurisées ou les moyens de traitement des informations sensibles, il convient d'accorder au personnel tiers chargé de l'assistance technique un accès limité, et uniquement sur demande de sa part. Il convient d'attribuer des habilitations pour cet accès et de le surveiller;

e) il convient de réexaminer et de mettre à jour régulièrement les droits d'accès aux zones sécurisées et de les supprimer si nécessaire (voir 8.3.3).

9.1.3 Sécurisation des bureaux, des salles et des équipements

Mesure

Il convient de concevoir et d'appliquer des mesures de sécurité physique pour les bureaux, les salles et les équipements.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes sur la sécurisation des bureaux, des salles et des équipements:

a) il convient de tenir compte des règlements et normes applicables en matière de santé et de sécurité des personnes;

b) pour les équipements-clés, il convient de choisir un emplacement non accessible au public;

c) dans la mesure du possible, il convient que les bâtiments soient d'une grande discrétion et donnent le minimum d'indications sur leur finalité, sans signe manifeste, extérieur ou intérieur, qui permette d'identifier la présence d'activités de traitement de l'information;

d) il convient que les répertoires et annuaires téléphoniques internes permettant d'identifier l'emplacement des moyens de traitement des informations sensibles ne soient pas aisément accessibles au public.

9.1.4 Protection contre les menaces extérieures et environnementales

Mesure

Il convient de concevoir et d'appliquer des mesures de protection physique contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistres provoqués par l'homme.

Préconisations de mise en œuvre

Il convient de prendre en considération toute menace contre la sécurité que pourraient présenter les locaux voisins, comme un incendie dans un bâtiment voisin, une fuite d'eau au plafond, une inondation dans les étages du sous-sol ou une explosion dans la rue.

Il convient de tenir compte des directives suivantes pour éviter les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistres provoqués par l'homme.

a) il convient de stocker les matières dangereuses ou combustibles à une distance suffisante d'une zone sécurisée. Il convient de ne pas stocker les fournitures en vrac, par exemple le papier, à l'intérieur d'une zone sécurisée;

b) il convient de placer le matériel de secours et les supports de sauvegarde à une distance de sécurité pour éviter tout dommage engendré par un sinistre touchant le site principal;

c) il convient de prévoir et de placer à un endroit approprié le matériel de lutte contre l'incendie.

9.1.5 Travail dans les zones sécurisées

Mesure

Il convient de concevoir et d'appliquer des mesures de protection physique et des directives pour le travail en zone sécurisée.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes:

a) concernant l'existence de zones sécurisées ou des activités qui s'y pratiquent, il convient que le personnel soit informé sur la seule base du besoin d'en connaître;

b) en zone sécurisée, il convient d'éviter le travail non encadré tant pour des raisons de sécurité des personnes que pour prévenir toute occasion d'acte malveillant;

c) il convient de verrouiller physiquement et de contrôler périodiquement les zones sécurisées inoccupées;

d) il convient d'interdire les matériels photographique, vidéo, audio ou autres matériels d'enregistrement comme les appareils photos intégrés à des appareils mobiles, sauf autorisation expresse;

Les dispositions relatives au travail en zone sécurisée prévoient des mesures applicables aux salariés, contractants et utilisateurs tiers rattachés aux zones sécurisées, aussi bien qu'aux autres tiers intervenant dans ces zones.

9.1.6 Zones d'accès public, de livraison et de chargement

Mesure

Il convient de contrôler les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux. Il convient également d'isoler les points d'accès, si possible, des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes:

a) il convient que l'accès à une zone de livraison/chargement depuis l'extérieur du bâtiment soit limité au personnel identifié et habilité;

b) il convient de concevoir la zone de livraison/chargement de sorte que les marchandises reçues puissent être déchargées sans que le personnel de livraison n'ait accès aux autres parties du bâtiment;

c) il convient de sécuriser les portes extérieures d'une zone de livraison/chargement lorsque les portes intérieures sont ouvertes;

d) il convient d'inspecter les matières entrantes pour vérifier l'absence de menaces potentielles [voir 9.2.1d)] avant le transfert de ces matières de la zone de livraison/chargement à leur point d'utilisation;

e) il convient d'enregistrer les matières entrantes conformément aux procédures de gestion des biens (voir également 7.1.1) au moment de leur entrée sur le site;

f) dans la mesure du possible, il convient de séparer physiquement les chargements entrants des chargements sortants.

9.2 Sécurité du matériel

Objectif: empêcher la perte, l'endommagement, le vol ou la compromission des biens et l'interruption des activités de l'organisme.

Il convient de protéger le matériel des menaces physiques et environnementales.

La protection du matériel (incluant le matériel utilisé hors site et la sortie d'un matériel) est nécessaire pour réduire les risques d'accès non autorisé à l'information et se prémunir contre la perte et les dommages. Il convient de prendre également en compte le choix de l'emplacement et la mise au rebut du matériel. Des mesures particulières peuvent être requises pour préserver les installations électriques (alimentation et câblage) en les protégeant des menaces physiques.

9.2.1 Choix de l'emplacement et protection du matériel

Mesure

Il convient de situer et de protéger le matériel de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes pour protéger le matériel:

a) pour le matériel, il convient de choisir un emplacement permettant de réduire le plus possible les accès inutiles aux zones de travail;

b) il convient de choisir la position des moyens de traitement de l'information manipulant des données sensibles et d'en limiter l'angle de vue pour réduire le risque que ces informations soient vues par des personnes non habilitées, et il convient de sécuriser les équipements de stockage pour éviter un accès non autorisé;

c) il convient d'isoler les éléments nécessitant une protection particulière afin de pouvoir abaisser le niveau général de protection requise;

d) il convient d'adopter des mesures visant à réduire le plus possible les risques de menaces physiques potentielles, comme le vol, l'incendie, les explosifs, la fumée, les fuites d'eau (ou une rupture de l'alimentation en eau), la poussière, les vibrations, les effets engendrés par les produits chimiques, les interférences sur le secteur électrique, les interférences sur les lignes de télécommunication, les rayonnements électromagnétiques et le vandalisme;

e) il convient de fixer des directives sur le fait de manger, boire et fumer à proximité des moyens de traitement de l'information;

f) il convient de surveiller les conditions ambiantes, telles que la température et l'humidité, qui pourraient nuire au fonctionnement des moyens de traitement de l'information;

g) il convient d'appliquer une protection contre la foudre à l'ensemble des bâtiments et il convient d'équiper de filtres antifoudre toutes les lignes électriques et de télécommunication entrantes;

h) il convient d'envisager l'utilisation de méthodes spéciales de protection, telles que les claviers à membrane, pour le matériel en environnement industriel;

i) il convient de protéger les moyens de traitement de l'information sensibles pour réduire le plus possible les risques de fuites d'informations dues aux émissions électromagnétiques.

9.2.2 Services généraux

Mesure

Il convient de protéger le matériel des coupures de courant et autres perturbations dues à une défaillance des services généraux.

Préconisations de mise en œuvre

Il convient que tous les services généraux, tels que l'électricité, l'alimentation en eau, l'évacuation des eaux usées, le chauffage/la ventilation et la climatisation soient correctement dimensionnés pour les systèmes pris en charge. Il convient d'inspecter régulièrement et, le cas échéant, de soumettre à essai les services généraux pour s'assurer de leur bon fonctionnement et pour écarter tout risque de dysfonctionnement ou de panne. Il convient d'installer une alimentation électrique adaptée, conforme aux spécifications du fabricant du matériel.

L'utilisation d'un onduleur gérant l'arrêt normal ou le fonctionnement en continu est recommandée pour le matériel prenant en charge des opérations critiques pour l'organisme. Il convient que les plans de secours de l'alimentation électrique prévoient l'action à entreprendre en cas de panne de l'onduleur. Il convient d'envisager l'emploi d'un générateur de secours si le traitement doit continuer en cas de coupure de courant prolongée. Il convient de prévoir une quantité de carburant suffisante pour garantir le bon fonctionnement du générateur pendant une période prolongée. Il convient de vérifier l'onduleur et les générateurs régulièrement pour s'assurer qu'ils possèdent la capacité suffisante, conformément aux recommandations du fabricant. En outre, il peut être envisagé d'utiliser plusieurs sources d'alimentation ou, si le site est vaste, une sous-station électrique autonome.

Il convient de placer les disjoncteurs d'urgence près des sorties de secours des salles abritant les matériels pour faciliter une mise hors tension rapide en cas d'urgence. Il convient de prévoir un éclairage de secours en cas de coupure de l'alimentation principale.

Il convient que l'alimentation en eau soit régulière et suffisante pour alimenter les systèmes de climatisation, d'humidification et de lutte contre les incendies (le cas échéant). Des dysfonctionnements dans le système d'alimentation en eau peuvent endommager le matériel ou empêcher les extincteurs de fonctionner efficacement. Il convient d'évaluer l'intérêt d'un système d'alarme qui détecte les dysfonctionnements des services généraux et de procéder, si nécessaire, à son installation.

Il convient de connecter l'infrastructure de télécommunications à l'opérateur téléphonique par au moins deux voies différentes pour empêcher que la défaillance d'une voie de connexion ne supprime le service voix. Il convient que le service voix soit de qualité suffisante pour satisfaire aux exigences légales locales en matière d'appels d'urgence.

Informations supplémentaires

Les sources d'alimentation multiples sont une option pour éviter l'existence d'un point unique de faiblesse.

9.2.3 Sécurité du câblage

Mesure

Il convient de protéger les câbles électriques ou de télécommunications transportant des données contre toute interception ou dommage.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes sur la sécurité du câblage:

a) il convient d'enterrer, dans la mesure du possible, les lignes électriques et les lignes de télécommunication branchées aux moyens de traitement de l'information ou de les soumettre à toute autre forme de protection adéquate;

b) il convient de protéger le câblage réseau contre les interceptions non autorisées ou les dommages en utilisant, par exemple, un conduit de câbles ou en évitant que les voies traversent des zones publiques;

c) il convient de séparer les câbles électriques et les câbles de télécommunication pour éviter toute interférence;

d) il convient d'utiliser un marquage clairement identifiable sur les câbles et les matériels pour réduire le plus possible les erreurs de manipulation, telles qu'un raccordement accidentel des mauvais câbles réseau;

e) il convient d'utiliser une liste documentée des raccordements à effectuer pour réduire les possibilités d'erreurs;

f) pour les systèmes sensibles ou critiques, les mesures supplémentaires à envisager comprennent les aspects suivants:

    1) l'installation d'un conduit de câbles blindé et de salles ou box verrouillés aux points d'inspection et aux extrémités;

2) l'utilisation de routages et/ou de moyens de transmission alternatifs offrant un niveau de sécurité adéquat;

3) l'utilisation de câbles en fibre optique;

4) l'utilisation d'un blindage protégeant les câbles contre les interférences électromagnétiques;

5) le déclenchement de balayages techniques et d'inspections physiques contre les appareils non autorisés branchés sur les câbles;

6) un accès contrôlé aux panneaux de raccordements et aux salles des câbles;

9.2.4 Maintenance du matériel

Mesure

Il convient d'entretenir le matériel correctement pour garantir sa disponibilité permanente et son intégrité.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes sur la maintenance du matériel:

a) il convient d'entretenir le matériel conformément aux spécifications et aux intervalles de dépannage recommandés par le fournisseur;

b) il convient que seul le personnel habilité effectue des réparations et dépanne le matériel;

c) il convient de conserver un dossier de toutes les pannes suspectées ou avérées et de toutes les tâches de maintenance préventive ou correctives;

d) il convient de mettre en œuvre les mesures adéquates lorsque la maintenance d'un matériel est planifiée, en s'interrogeant pour savoir si elle a été effectuée par du personnel sur site ou extérieur à l'organisme; lorsque cela est nécessaire, il convient que les informations sensibles contenues dans le matériel aient été effacées ou que le personnel de maintenance ait reçu les autorisations suffisantes;

e) il convient de respecter toutes les exigences qu'imposent les polices d'assurance.

9.2.5 Sécurité du matériel hors des locaux

Mesure

Il convient d'appliquer la sécurité au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site.

Préconisations de mise en œuvre

Il convient que ce soit la direction qui autorise l'utilisation de matériels de traitement de l'information hors des locaux de l'organisme, sans tenir compte de qui en est le propriétaire.

Il convient de prendre en compte les directives suivantes concernant la protection du matériel hors site:

a) il convient de ne pas laisser le matériel et les supports de données sortis des locaux sans surveillance dans des espaces publics; il convient de transporter les ordinateurs portables comme des bagages à main et de les dissimuler autant que possible lors des déplacements;

b) il convient d'observer à tout instant les instructions du fabricant visant à protéger le matériel, par exemple celle sur la protection contre les champs électromagnétiques forts;

c) il convient de décider des mesures relatives au travail à domicile par une appréciation du risque et d'appliquer, le cas échéant, les mesures adaptées, par exemple des armoires à fichiers fermant à clé, une politique de bureaux propres, des contrôles d'accès aux ordinateurs et une communication sécurisée avec le bureau (voir également l'ISO/CEI 18028-4 concernant la sécurité des réseaux);

d) il convient de prévoir des garanties d'assurance adéquates pour protéger le matériel hors site.

Il convient de tenir compte des risques pour la sécurité comme les dommages, le vol ou les écoutes, qui peuvent varier considérablement suivant les lieux, pour déterminer les mesures les plus adéquates.

Informations supplémentaires

Les matériels de stockage et de traitement de l'information comprennent tous types d'ordinateurs individuels, d'agendas électroniques, de téléphones mobiles, de cartes à puce, de papier ou autre appareil, utilisé pour travailler à domicile ou être transporté hors du lieu de travail habituel.

Pour plus ample information sur les autres aspects de la protection du matériel mobile, voir 11.7.1.

9.2.6 Mise au rebut ou recyclage sécurisé(e) du matériel

Mesure

Il convient de vérifier tout le matériel contenant des supports de stockage soient vérifiées pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut.

Préconisations de mise en œuvre

Il convient de détruire physiquement les appareils contenant des informations sensibles ou de détruire, supprimer ou écraser les informations au moyen de techniques empêchant de retrouver l'information d'origine plutôt que par la fonction standard de suppression ou de formatage.

Informations supplémentaires

Les appareils endommagés contenant des données sensibles peuvent nécessiter une appréciation du risque visant à déterminer s'il convient de les détruire physiquement plutôt que de les envoyer en réparation ou de les mettre au rebut.

L'information peut être compromise par une mise au rebut ou un recyclage imprudent(e) du matériel (voir également 10.7.2).

9.2.7 Sortie d'un bien

Mesure

Il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisme sans autorisation préalable.

Préconisations de mise en œuvre

Il convient de tenir compte des directives suivantes:

a) il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisme sans autorisation préalable;

b) il convient d'identifier clairement les salariés, contractants et utilisateurs tiers qui ont autorité pour permettre la sortie de biens hors du site. Les dispositions relatives au travail en zone sécurisée comprennent des mesures applicables aux salariés, contractants et utilisateurs tiers rattachés aux zones sécurisées, aussi bien qu'aux autres tiers intervenant dans ces zones.

c) il convient de fixer des délais pour la sortie de matériels et de vérifier que ces délais ont été respectés lorsque le matériel est rendu;

d) le cas échéant, il convient d'enregistrer la sortie du matériel et son retour dans les locaux de l'organisme.

Informations supplémentaires

Des contrôles ponctuels, destinés à détecter une sortie de bien non autorisée, peuvent aussi servir à détecter les appareils d'enregistrement non autorisés, les armes, etc. et empêcher qu'ils pénètrent dans le site. Il convient d'effectuer ces contrôles ponctuels conformément à la législation et aux règlements applicables. Il convient d'informer les personnes de la tenue d'un contrôle ponctuel, et il convient de réaliser ces contrôles uniquement après obtention d'une autorisation conforme aux exigences légales et réglementaires.

10 Gestion de l'exploitation et des télécommunications

10.1 Procédures et responsabilités liées à l'exploitation

Objectif: assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.

Il convient d'établir les responsabilités et les procédures liées à la gestion et l'exploitation de l'ensemble des moyens de traitement de l'information. Cela comprend la mise au point de procédures d'exploitation appropriées.

Il convient de mettre en œuvre, le cas échéant, une séparation des tâches pour réduire les risques de mauvais usage du système, qu'il s'agisse d'une négligence ou d'un acte délibéré.

10.1.1 Procédures d'exploitation documentées

Mesure

Il convient que les procédures d'exploitation soient documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.

Préconisations de mise en œuvre

Il convient de documenter des procédures pour les activités du système liées aux moyens de traitement de l'information et de télécommunication, telles que les procédures de démarrage/arrêt de l'ordinateur, la sauvegarde, la maintenance du matériel, la manipulation des supports, la gestion du courrier et de la salle des ordinateurs, et la sécurité des personnes.

Il convient que les procédures d'exploitation précisent les instructions à suivre pour l'exécution de chaque tâche, dont les suivantes:

a) traitement et manipulation des informations;

b) sauvegarde (voir 10.5);

c) exigences de planification, y compris les interdépendances avec d'autres systèmes et les heures de début de première tâche et de fin de dernière tâche;

d) instructions pour gérer les erreurs ou autres conditions exceptionnelles susceptibles d'apparaître lors de l'exécution de la tâche, y compris les restrictions sur l'emploi des utilitaires système (voir 11.5.4);

e) contacts avec l'assistance technique en cas de difficultés techniques ou d'exploitation inattendues;

f) instructions particulières sur la manipulation des supports et des données de sortie, telles que l'utilisation de papiers spéciaux ou la gestion de données de sortie confidentielles, qui comprennent des procédures d'élimination sécurisée des données de sortie issues de tâches ayant échoué (voir 10.7.2 et 10.7.3);

g) procédures de redémarrage et de récupération du système à appliquer en cas de panne du système;

h) gestion des informations contenues dans les traces d'audit et les journaux système (voir 10.10).

Il convient que les procédures d'exploitation et les procédures documentées s'appliquant aux activités du système soient traitées comme des documents formels et que les modifications apportées soient autorisées par la direction. Lorsque cela est techniquement réalisable, il convient de gérer les systèmes d'information de façon homogène par le biais de procédures, outils et utilitaires identiques.

10.1.2 Gestion des modifications

Mesure

Il convient de contrôler les changements apportés aux systèmes et moyens de traitement de l'information.

Préconisations de mise en œuvre

Il convient de soumettre les systèmes en exploitation et les logiciels d'application à un contrôle strict de la gestion des modifications. Il convient d'envisager en particulier les éléments suivants:

a) identifier et consigner les changements importants;

b) planifier les changements et les soumettre à essai;

c) évaluer les impacts potentiels de ces changements, y compris les impacts sur la sécurité;

d) établir une procédure d'accord formel pour les changements proposés;

e) transmettre les informations détaillées sur les changements apportés à toutes les personnes concernées;

f) définir des procédures de repli, incluant les procédures et les responsabilités en cas d'abandon et de récupération suite à l'échec des changements ou à des événements imprévus.

Il convient de mettre en place des procédures et des responsabilités de gestion formelles pour assurer un contrôle satisfaisant de tous les changements apportés aux matériels, logiciels ou procédures. Lorsque des changements sont effectués, il convient de conserver un rapport d'audit contenant toutes les informations pertinentes.

Informations supplémentaires

Un contrôle insuffisant des changements apportés aux systèmes et moyens de traitement de l'information constitue une cause courante de défaillance du système ou de la sécurité. Une modification de l'environnement d'exploitation, particulièrement s'il s'agit de faire passer un système du stade de développement au stade d'exploitation, peut avoir un impact sur la fiabilité des applications (voir également 12.5.1).

Il convient de n'apporter des changements aux systèmes en exploitation que pour des raisons valables, liées à l'activité, par exemple en cas d'accroissement du risque pour le système. La mise à niveau des systèmes avec les dernières versions des systèmes d'exploitation ou des applications n'est pas toujours dans l'intérêt de l'organisme, car cela est susceptible d'introduire davantage de vulnérabilités et d'instabilité qu'avec la version actuelle. Cela peut signifier également des coûts supplémentaires en termes de formation, de licences, d'assistance technique, de maintenance et de frais administratifs, sans oublier les besoins en nouveau matériel, particulièrement lors de la migration.

10.1.3 Séparation des tâches

Mesure

Il convient de séparer les tâches et les domaines de responsabilité pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des biens de l'organisme.

Préconisations de mise en œuvre

La séparation des tâches est une méthode pour diminuer les risques de mauvais usage accidentel ou délibéré du système. Il convient de prendre garde que personne n'ait accès, ne modifie ou n'utilise des biens sans en avoir l'autorisation ou sans avoir été détecté. Il convient de séparer le moment de l'événement du moment de son autorisation. Il convient d'envisager la possibilité de collusion lors de la conception des mesures.

Les organismes de petite taille peuvent avoir des difficultés pour séparer les tâches, mais il convient d'appliquer ce principe dans la mesure du possible. Lorsqu'il est difficile de procéder à la séparation des tâches, il convient d'envisager d'autres mesures comme la surveillance des activités, les traces d'audit et l'encadrement par la direction. Il est important que l'audit de sécurité reste indépendant.

10.1.4 Séparation des équipements de développement, de test et d'exploitation

Mesure

Il convient de séparer les équipements de développement, de test et d'exploitation pour réduire les risques d'accès ou de changements non autorisés dans le système en exploitation.

Préconisations de mise en œuvre

Il convient de déterminer le niveau de séparation nécessaire entre les environnements d'exploitation, de test et de développement pour prévenir les problèmes d'exploitation et mettre en œuvre les mesures appropriées.

Il convient d'envisager les directives suivantes:

a) il convient de définir et de documenter les règles concernant le passage des logiciels du stade de développement au stade d'exploitation;

b) il convient d'exécuter les logiciels de développement et les logiciels d'exploitation sur des ordinateurs (systèmes ou microprocesseurs) différents et dans des domaines ou répertoires différents;

c) il convient que les compilateurs, éditeurs et autres outils de développement ou utilitaires système ne soient accessibles depuis les systèmes en exploitation que lorsque cela est nécessaire;

d) il convient que l'environnement du système de test émule aussi rigoureusement que possible l'environnement du système en exploitation;

e) il convient que les utilisateurs utilisent des profils utilisateurs différents pour les systèmes en exploitation et les systèmes de test et que les menus affichent les messages d'identification adéquats pour réduire le risque d'erreur;

f) il convient que les données sensibles ne soient pas copiées dans l'environnement du système de test (voir 12.4.2).

Informations supplémentaires

Les activités liées au développement et au test peuvent causer de graves problèmes, tels qu'une modification indésirable des fichiers ou de l'environnement système, ou une panne du système. Dans ce cas, il est nécessaire de maintenir un environnement stable et connu de tous permettant de réaliser les tests significatifs. Il est également nécessaire d'empêcher tout accès inapproprié des développeurs.

Lorsque les personnels de développement et de test ont accès au système en exploitation et aux informations qu'il renferme, ils risquent d'y introduire du code non autorisé ou non soumis à essai ou de modifier les données d'exploitation. Sur certains systèmes, cette possibilité pourrait être utilisée à mauvais escient pour commettre une fraude ou introduire du code non soumis à essai ou malveillant, ce qui pourrait créer de graves problèmes d'exploitation.

Les développeurs et les personnes chargées des tests représentent également une menace pour la confidentialité des informations d'exploitation. Les activités de développement et de test peuvent entraîner des changements involontaires dans les logiciels ou les informations si elles partagent le même environnement informatique. La séparation physique des équipements de développement, de test et d'exploitation est donc souhaitable pour réduire les risques de changements accidentels ou d'accès non autorisé aux logiciels d'exploitation et aux données liées à l'activité (voir également 12.4.2 pour la protection des données d'essai).

10.2 Gestion de la prestation de service par un tiers

Objectif: mettre en œuvre et maintenir un niveau de sécurité de l'information et de service adéquat et conforme aux accords de prestation de service par un tiers.

Il convient que l'organisme vérifie la mise en œuvre des accords, contrôle leur exécution et gère les changements pour veiller à ce que les services fournis répondent à toutes les exigences ayant fait l'objet d'un accord avec le tiers.

10.2.1 Prestation de service

Mesure

Il convient de s'assurer que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers.

Préconisations de mise en œuvre

Il convient que la prestation de service par un tiers satisfasse aux dispositions de sécurité, aux définitions de service et aux modalités de gestion du service prévues dans l'accord. Dans le cas de dispositions relatives à l'externalisation, il convient que l'organisme planifie les transitions nécessaires (pour les informations, les moyens de traitement de l'information et tout ce qui transite en général) et qu'il s'assure que la sécurité est maintenue tout au long de la période de transition.

Il convient que l'organisme s'assure que le tiers maintient une capacité de service suffisante et qu'il dispose de plans réalisables pour veiller au respect des dispositions relatives à la continuité du service en cas de défaillance majeure du service ou de sinistre (voir 14.1).

10.2.2 Surveillance et réexamen des services tiers

Mesure

Il convient que les services, rapports et enregistrements fournis par les tiers soient régulièrement contrôlés et réexaminés, et que des audits soient régulièrement réalisés.

Préconisations de mise en œuvre

Il convient que la surveillance et le réexamen des services tiers garantissent le respect des conditions générales sur la sécurité de l'information prévues dans les accords et de la bonne gestion des incidents et problèmes liés à la sécurité de l'information. Il convient que cela implique une relation et un processus de gestion du service entre l'organisme et le tiers pour les tâches suivantes:

a) surveiller les niveaux de performance du service et vérifier ainsi qu'ils sont conformes aux accords;

b) réexaminer les rapports de service produits par le tiers et organiser des réunions régulières sur l'avancement comme l'exigent les accords;

c) fournir des informations sur les incidents liés à la sécurité de l'information et le réexamen de ces informations par le tiers/l'organisme comme l'exigent les accords et toute directive et procédure d'accompagnement;

d) réexaminer les traces d'audit et enregistrements du tiers concernant les événements relatifs à la sécurité, les problèmes d'exploitation, les défaillances et le suivi des pannes et interruptions liées au service fourni;

e) résoudre et gérer tout problème identifié.

Il convient d'attribuer la responsabilité de la relation avec le tiers à une personne désignée ou à une équipe. En outre, il convient que l'organisme s'assure que le tiers nomme les personnes chargées de contrôler le respect et la mise en application des exigences de l'accord. Il convient de prévoir les compétences et ressources techniques suffisantes pour veiller à ce que les exigences de l'accord (voir 6.2.3), et en particulier celles qui traitent de la sécurité de l'information, soient respectées. Il convient de prendre les mesures adéquates lorsque des insuffisances sont observées dans la prestation du service.

Il convient que l'organisme conserve une visibilité et un contrôle global et suffisant sur tous les aspects de la sécurité ayant trait à l'accès, au traitement ou à la gestion par un tiers d'informations ou de moyens de traitement de l'information sensibles ou critiques. Il convient que l'organisme veille à conserver, par un processus, un format et une structure de signalement clairement définis, une visibilité sur les activités liées à la sécurité, telles que la gestion des modifications, l'identification des vulnérabilités et le signalement des incidents liés à la sécurité de l'information et les réponses qui y sont apportées.

Informations supplémentaires

En cas d'externalisation, l'organisme doit savoir que la responsabilité ultime de l'information traitée par un tiers externe lui incombe.

10.2.3 Gestion des modifications dans les services tiers

Mesure

Il convient de gérer les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, en tenant compte de la criticité des systèmes et processus de gestion concernés et de la réévaluation du risque.

Préconisations de mise en œuvre

Les éléments à prendre en compte dans le processus de gestion des modifications dans les services tiers sont les suivants:

a) changements effectués par l'organisme pour mettre en œuvre ce qui suit:

   1) les améliorations à apporter aux services actuellement offerts;

   2) le développement d'applications et de systèmes nouveaux;

   3) la modification ou mise à jour des politiques et procédures de l'organisme;

   4) les mesures nouvelles pour résoudre les incidents liés à la sécurité de l'information et pour améliorer la sécurité;

b) changements effectués par le tiers pour mettre en œuvre ce qui suit:

   1) les changements et les améliorations à apporter aux réseaux;

   2) l'utilisation de nouvelles technologies;

   3) l'adoption de nouveaux logiciels ou de versions/éditions plus récentes,

   4) les outils et environnements de développement nouveaux;

   5) les changements dans l'emplacement des équipements de dépannage;

   6) le changement de fournisseurs.

10.3 Planification et acceptation du système

Objectif: réduire le plus possible le risque de pannes du système.

Une planification en amont est indispensable pour assurer la disponibilité des capacités et ressources appropriées en vue d'offrir les performances requises pour le système.

Il convient de faire des projections sur les futurs dimensionnements afin de réduire le risque de surcharge du système.

Il convient de définir les exigences relatives à l'exploitation des nouveaux systèmes, de les documenter et de les soumettre à essai avant leur acceptation et leur utilisation.

10.3.1 Dimensionnement

Mesure

Il convient de surveiller et d'ajuster au plus près l'utilisation des ressources et il convient de faire des projections sur les dimensionnements futurs pour assurer les performances requises pour le système.

Préconisations de mise en œuvre

Pour chaque activité nouvelle et en cours, il convient d'identifier le dimensionnement associé. Il convient d'appliquer un réglage et une surveillance du système pour assurer, et s'il y a lieu améliorer, la disponibilité et l'efficacité des systèmes. Il convient de mettre en place des mesures de détection pour identifier les problèmes en temps voulu. Il convient que les projections sur les futurs dimensionnements tiennent compte des nouvelles exigences métier et système, et des tendances actuelles et projetées concernant les capacités de traitement de l'information de l'organisme.

Il est nécessaire de porter une attention particulière aux ressources pour lesquelles les délais d'approvisionnement sont longs ou les coûts élevés; il convient donc que les responsables surveillent l'usage des ressources-clés du système. Il convient que les responsables identifient les tendances en termes d'usage, en particulier des applications de gestion ou des outils système de gestion de l'information.

Il convient que les responsables utilisent ces informations pour identifier et éviter les goulots d'étranglement potentiels, et pour éviter d'avoir à dépendre de personnel-clé, ce qui pourrait représenter une menace pour la sécurité du système ou pour les services. Il convient que les responsables planifient en conséquence l'action adéquate.

10.3.2 Acceptation du système

Mesure

Il convient de fixer les critères d'acceptation pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et de réaliser les tests adaptés du (des) système(s) au moment du développement et préalablement à leur acceptation.

Préconisations de mise en œuvre

Il convient pour les responsables de s'assurer que les exigences et les critères d'acceptation relatifs aux nouveaux systèmes sont clairement définis, convenus, documentés et soumis à essai. Il convient que les nouveaux systèmes d'information, nouvelles versions et mises à niveau soient passés en production uniquement après acceptation formelle. Il convient de prendre en compte les éléments suivants avant l'acceptation formelle:

a) les exigences en matière de performances et de capacité de l'ordinateur;

b) les procédures de reprise après erreur et de redémarrage du système ainsi que les plans de secours;

c) l'élaboration des procédures d'exploitation de routine selon des normes définies et les essais correspondants;

d) l'ensemble de mesures de sécurité mises en place et ayant fait l'objet d'un accord;

e) les procédures manuelles efficaces;

f) les dispositions relatives à la continuité de l'activité (voir 14.1);

g) les preuves démontrant que l'installation du nouveau système ne nuira pas aux systèmes existants, en particulier lors des pics de traitement, comme la fin du mois;

h) les preuves démontrant que l'effet du nouveau système sur la sécurité globale de l'organisme a été analysé;

i) la formation sur l'exploitation ou l'utilisation des nouveaux systèmes;

j) la facilité d'utilisation, puisqu'elle influe sur les performances de l'utilisateur et permet d'éviter les erreurs humaines.

Pour les nouveaux développements majeurs, il convient de consulter les utilisateurs et les personnes occupant des fonctions opérationnelles à tous les stades du processus de développement pour assurer l'efficacité opérationnelle de la conception système proposée. Il convient de mener les essais appropriés pour confirmer que tous les critères d'acceptation ont été entièrement satisfaits.

Informations supplémentaires

L'acceptation peut comprendre un processus formel de certification et d'agrément pour vérifier que les exigences en matière de sécurité sont satisfaites.

10.4 Protection contre les codes malveillant et mobile

Objectif: protéger l'intégrité des logiciels et de l'information.

Des précautions sont requises pour prévenir et détecter l'introduction de code malveillant et de code mobile non autorisé.

Les logiciels et les moyens de traitement de l'information sont vulnérables à l'introduction de code malveillant comme les virus informatiques, les vers de réseau, les chevaux de Troie et les bombes logiques. Il convient d'informer les utilisateurs des dangers des codes malveillants. Il convient que les responsables introduisent des mesures, le cas échéant, pour prévenir, détecter et supprimer les codes malveillants et contrôler le code mobile.

10.4.1 Mesures contre les codes malveillants

Mesure

Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs.

Préconisations de mise en œuvre

Il convient de fonder la protection contre les codes malveillants sur les logiciels de détection/réparation de code malveillant, la sensibilisation à la sécurité et les mesures adéquates de gestion des modifications et de l'accès au système. Il convient d'envisager les directives suivantes:

a) établir une politique formelle prohibant l'utilisation de logiciels non autorisés (voir 15.1.2);

b) établir une politique formelle indiquant les mesures de protection qu'il convient de prendre pour se protéger des risques liés aux fichiers et logiciels obtenus aussi bien depuis ou via les réseaux externes que sur tout autre support;

c) mener des réexamens réguliers des logiciels et du contenu des données des systèmes traitant des processus critiques pour l'activité; il convient de conduire une enquête formelle sur la présence de tout fichier non approuvé ou de modifications non autorisées;

d) l'installation et la mise à jour régulière, comme mesure de précaution ou tâche de routine, des logiciels de détection/réparation de code malveillant pour analyser les ordinateurs et les supports; il convient que les contrôles réalisés comprennent les tâches suivantes:

   1) vérification avant usage de l'absence de code malveillant dans tout fichier stocké sur un support électronique ou optique, ou reçu via les réseaux;

   2) vérification avant usage de l'absence de code malveillant dans les pièces jointes et les fichiers téléchargés; il convient de mener cette vérification à différents endroits, par exemple sur les serveurs de messagerie électronique, les ordinateurs de bureau et à l'entrée du réseau de l'organisme;

   3) vérification de l'absence de code malveillant dans des pages web;

e) la définition de procédures et de responsabilités de gestion abordant la protection des systèmes contre les codes malveillants, la formation à l'utilisation de ces systèmes, et le signalement et la récupération après une attaque par code malveillant (voir 13.1 et 13.2);

f) l'élaboration des plans appropriés de continuité de l'activité pour la récupération après une attaque par code malveillant, comprenant toutes les données nécessaires, les sauvegardes logicielles et les dispositions de récupération (voir Article 14);

g) la mise en œuvre de procédures pour recueillir régulièrement des informations, comme l'inscription à des listes de diffusion et/ou la consultation de sites web donnant des informations sur les nouveaux codes malveillants;

h) la mise en œuvre de procédures pour vérifier les informations en rapport avec les codes malveillants et s'assurer que les bulletins d'alerte sont exacts et informatifs; il convient que les responsables veillent à l'utilisation de sources qualifiées: publications réputées, sites Internet fiables ou éditeurs de logiciels de protection contre les codes malveillants pour faire la différence entre les canulars et une menace réelle; il convient d'informer tous les utilisateurs du problème des canulars et de la marche à suivre s'ils en reçoivent.

Informations supplémentaires

L'utilisation sur l'ensemble de l'environnement de traitement de l'information d'au moins deux logiciels de protection contre les codes malveillants provenant d'éditeurs différents peut accroître l'efficacité de la protection contre les codes malveillants.

Les logiciels de protection contre les codes malveillants peuvent être installés pour permettre la mise à jour automatique des fichiers de définition et des moteurs d'analyse afin de garantir que la protection est à jour. En outre, il est possible d'installer ces logiciels sur tous les ordinateurs de bureau pour effectuer des vérifications automatiques.

Il convient de veiller à se protéger de l'introduction de code malveillant au cours des procédures de maintenance et d'urgence, qui peuvent court-circuiter les mesures habituelles de protection contre les codes malveillants.

10.4.2 Mesures contre le code mobile

Mesure

Lorsque l'utilisation de code mobile est autorisée, il convient que la configuration garantisse que le code mobile fonctionne selon une politique de sécurité clairement définie et il convient d'empêcher tout code mobile non autorisé de s'exécuter.

Préconisations de mise en œuvre

Pour se protéger d'un code mobile lançant des actions non autorisées, il convient d'envisager les actions suivantes:

a) exécuter le code mobile dans un environnement isolé logiquement;

b) bloquer toute utilisation de code mobile;

c) bloquer la réception de code mobile;

d) mettre en pratique les mesures techniques disponibles sur un système donné pour garantir le traitement du code mobile;

e) contrôler les ressources accessibles au code mobile;

f) utiliser des moyens cryptographiques pour authentifier de façon exclusive le code mobile.

Informations supplémentaires

Un code mobile est un code logiciel qui se transfère d'un ordinateur à un autre pour s'exécuter automatiquement et réaliser une action spécifique avec peu ou pas du tout d'interaction de l'utilisateur. On associe le code mobile à de nombreux services de la couche intermédiaire.

Hormis pour s'assurer que le code mobile ne contient pas de code malveillant, le contrôle de code mobile est aussi essentiel pour éviter une utilisation non autorisée ou une interruption du système, du réseau ou des ressources de l'application ainsi que les brèches dans la sécurité de l'information.

10.5 Sauvegarde

Objectif: maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.

Il convient de dresser des procédures de routine pour mettre en œuvre la politique et la stratégie de sauvegarde convenues (voir également 14.1) stipulant de réaliser des copies de sauvegarde des données et de procéder à des répétitions pour que leur restauration puisse être effectuée en temps voulu.

10.5.1 Sauvegarde des informations

Mesure

Il convient de réaliser des copies de sauvegarde des informations et logiciels et de les soumettre régulièrement à essai conformément à la politique de sauvegarde convenue.

Préconisations de mise en œuvre

Il convient de fournir les équipements de sauvegarde adéquats pour s'assurer que l'ensemble des informations et logiciels essentiels pourront être récupérés en cas de sinistre ou de défaillance d'un support.

Pour la sauvegarde des informations, il convient de prendre en compte les éléments suivants:

a) il convient de définir le niveau de sauvegarde nécessaire;

b) il convient de produire des enregistrements exacts et complets des copies de sauvegarde ainsi que des procédures de restauration documentées;

c) il convient que l'étendue des sauvegardes (par exemple sauvegarde totale ou différentielle) et leur fréquence reflète les exigences métier de l'organisme, les exigences relatives à la sécurité des informations concernées, et la criticité des informations pour la continuité de l'activité de l'organisme;

d) il convient de placer les sauvegardes à un endroit suffisamment éloigné pour échapper aux dommages d'un sinistre sur le site principal;

e) il convient de donner aux informations sauvegardées un niveau de protection physique et environnementale adéquat (voir Article 9) compatible avec les normes en vigueur sur le site principal; il convient d'étendre les mesures appliquées sur le site principal pour qu'elles couvrent aussi le site de sauvegarde;

f) il convient de soumettre régulièrement à essai les supports de sauvegarde pour s'assurer de leur fiabilité en cas d'utilisation en urgence;

g) il convient de vérifier régulièrement les procédures de restauration et de les soumettre à essai pour s'assurer qu'elles sont efficaces et qu'elles peuvent être menées à leur terme dans les délais prévus dans les procédures de récupération;

h) dans les situations où la confidentialité a une importance, il convient de protéger les sauvegardes en les chiffrant.

Il convient de soumettre régulièrement à essai les dispositions en matière de sauvegarde pour s'assurer de leur conformité avec les plans de continuité de l'activité (voir Article 14). Pour les systèmes critiques, il convient que les dispositions relatives aux sauvegardes traitent de tous les systèmes d'information, applications et données nécessaires à la récupération totale du système en cas de sinistre.

Il convient de déterminer la période de conservation des informations essentielles pour l'activité de l'organisme ainsi que toute nécessité de conserver les copies archivées de façon permanente (voir 15.1.3).

Informations supplémentaires

Les dispositions sur les sauvegardes peuvent être automatisées pour faciliter le processus de sauvegarde et de restauration. Il convient de soumettre à essai, suffisamment et à intervalles réguliers, ces solutions d'automatisation avant de les mettre en œuvre.

10.6 Gestion de la sécurité des réseaux

Objectif: assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle ils s'appuient.

La gestion sécurisée des réseaux pouvant couvrir la totalité de l'organisme, il est nécessaire de porter une attention particulière au flux de données, aux implications juridiques, à la surveillance et la protection.

Des mesures supplémentaires peuvent aussi être requises pour protéger les informations sensibles transmises sur les réseaux publics.

10.6.1 Mesures sur les réseaux

Mesure

Il convient de gérer et de contrôler les réseaux de manière adéquate pour qu'ils soient protégés des menaces et de maintenir la sécurité des systèmes et des applications utilisant le réseau, notamment les informations en transit.

Préconisations de mise en œuvre

Il convient que les administrateurs réseau mettent en œuvre les mesures nécessaires pour assurer la sécurité des informations sur les réseaux et la protection des services connectés contre les accès non autorisés. Il convient d'envisager en particulier ce qui suit:

a) le cas échéant, il convient de séparer la responsabilité d'exploitation des réseaux et celle de l'exploitation des ordinateurs (voir 10.1.3);

b) il convient de définir les responsabilités et les procédures pour la gestion des matériels distants, notamment les matériels situés dans les zones utilisateurs;

c) il convient de définir des mesures spéciales pour préserver la confidentialité et l'intégrité des données transmises sur les réseaux publics ou les réseaux sans fil et de protéger les systèmes et applications connectés (voir 11.4 et 12.3); des mesures spéciales peuvent aussi s'avérer nécessaires pour maintenir la disponibilité des services réseau et des ordinateurs connectés;

d) il convient d'appliquer la journalisation et la surveillance appropriées pour permettre l'enregistrement des actions relevant de la sécurité;

e) il convient de coordonner étroitement les activités de gestion à la fois pour optimiser le service fourni à l'organisme et pour s'assurer que les mesures sont appliquées de façon homogène à travers toute l'infrastructure de traitement de l'information.

Informations supplémentaires

Pour des informations supplémentaires sur la sécurité des réseaux, voir l'ISO/CEI 18028, *Technologies de l'information — Techniques de sécurité — Sécurité de réseaux TI*.

10.6.2 Sécurité des services réseau

Mesure

Pour tous les services réseau, il convient d'identifier les fonctions réseau, les niveaux de service et les exigences de gestion, et de les intégrer dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.

Préconisations de mise en œuvre

Il convient de déterminer et de surveiller régulièrement la capacité du fournisseur de service réseau à gérer les services en question de façon sécurisée et il convient de se mettre d'accord sur le droit à auditer.

Il convient d'identifier les dispositions de sécurité nécessaires à des services en particulier, telles que les fonctions de sécurité, les niveaux de service et les exigences de gestion. Il convient que l'organisme veille à la mise en œuvre de ces mesures par les fournisseurs de services réseau.

Informations supplémentaires

Les services réseau comprennent la fourniture de connexions, les services de réseau privé, les réseaux à valeur ajoutée et les solutions de sécurité de gestion de réseaux comme les pare-feux et les systèmes de détection d'intrus. Ces services peuvent aller du simple octroi d'une bande passante non gérée aux offres complexes à valeur ajoutée.

On peut trouver ce qui suit parmi les fonctions de sécurité des services réseau:

a) la technologie s'appliquant à la sécurité des services réseau, comme l'authentification, le chiffrement et les contrôles de connexion au réseau;

b) les paramètres techniques requis pour la sécurisation de la connexion aux services réseau, conformément aux règles sur la sécurité et la connexion au réseau;

c) les procédures d'utilisation des services réseau pour restreindre, le cas échéant, l'accès des services ou applications réseau.

10.7 Manipulation des supports

Objectif: empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de biens et l'interruption des activités de l'organisme.

Il convient de contrôler et de protéger physiquement les supports.

Il convient d'établir des procédures d'exploitation adéquates pour protéger les documents, supports informatiques (bandes ou disquettes par exemple), les données saisies ou sorties et la documentation système contre la divulgation, la modification, le retrait et la destruction non autorisés.

10.7.1 Gestion des supports amovibles

Mesure

Il convient de mettre en place des procédures pour la gestion des supports amovibles.

Préconisations de mise en œuvre

Il convient de tenir compte des directives suivantes concernant la gestion des supports amovibles:

a) il convient de rendre impossible toute récupération du contenu d'un support recyclable devant être sorti de l'organisme, s'il n'est plus indispensable;

b) si nécessaire et réalisable, il convient d'exiger une autorisation pour la sortie de supports de l'organisme et de garder un enregistrement de ces sorties pour assurer la traçabilité;

c) il convient de stocker tous les supports dans un environnement sûr, sécurisé et conforme aux spécifications du fabricant;

d) il convient que les informations stockées sur supports qui nécessitent une disponibilité plus longue que la durée de vie de leur support (mentionnée dans les spécifications du fabricant) soient également stockées à un autre endroit, en vue d'éviter la perte d'informations due à la détérioration du support;

e) il convient d'envisager de tenir un registre des supports amovibles pour limiter les risques de perte de données;

f) il convient de n'activer des lecteurs de supports amovibles que si l'activité le nécessite.

Il convient de documenter clairement toutes les procédures et les niveaux d'autorisation.

Informations supplémentaires

Les supports amovibles comprennent les bandes DAT, les disquettes, les disques de mémoire flash, les disques durs amovibles, les CD, les DVD et les supports imprimés.

10.7.2 Mise au rebut des supports

Mesure

Il convient de mettre au rebut de façon sûre les supports qui ne servent plus, en suivant des procédures formelles.

Préconisations de mise en œuvre

Il convient que les procédures formelles pour la mise au rebut sécurisée des supports réduise le plus possible les fuites d'informations vers des personnes non habilitées. Il convient que les procédures de mise au rebut sécurisée des supports contenant des informations sensibles soient adaptées à la sensibilité de ces informations. Il convient d'envisager les directives suivantes:

a) il convient de stocker les supports contenant des informations sensibles et de les mettre au rebut de façon sûre et sécurisée, par exemple par incinération ou déchiquetage, ou d'en effacer les données pour qu'ils puissent resservir dans d'autres applications de l'organisme;

b) il convient de mettre en place les procédures pour identifier les éléments qui pourraient nécessiter une mise au rebut sécurisée;

c) il peut être plus facile de s'organiser pour collecter et mettre au rebut tous les supports de façon sécurisée que d'entreprendre de mettre à part les supports sensibles;

d) de nombreux organismes offrent des services de collecte et d'enlèvement des papiers, matériels et supports; il convient de sélectionner avec soin l'entrepreneur adapté disposant des mesures de sécurité et de l'expérience suffisants;

e) il convient, dans la mesure du possible, de journaliser la mise au rebut de pièces sensibles afin de tenir à jour la trace d'audit.

Lors de l'accumulation de supports en vue de leur mise au rebut, il convient de prendre en compte l'effet d'agrégation qui peut faire qu'une grande quantité d'informations non sensible devienne sensible.

Informations supplémentaires

Des informations sensibles sont susceptibles d'être divulguées du fait d'une mise au rebut négligente des supports (voir également 9.2.6 pour des informations sur la mise au rebut des matériels).

10.7.3 Procédures de manipulation des informations

Mesure

Il convient d'établir des procédures de manipulation et de stockage des informations pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage.

Préconisations de mise en œuvre

Il convient de rédiger des procédures spécifiant comment manipuler, traiter, stocker et communiquer les informations en fonction de leur classification (voir 7.2). Il convient d'envisager les éléments suivants:

a) manipuler et étiqueter tous les supports selon le niveau de classification indiqué;

b) restreindre les accès pour empêcher l'accès de personnes non habilitées;

c) tenir à jour un enregistrement formel des personnes habilitées pour être destinataires des données;

d) s'assurer que les données d'entrée sont complètes, que le traitement s'est correctement achevé et que la validation des données de sortie a été réalisée;

e) protéger les données en attente de sortie selon des niveaux correspondant à leur sensibilité;

f) stocker les supports conformément aux spécifications du fabricant;

g) réduire le plus possible la distribution des données;

h) marquer clairement toutes les copies de support du nom de la personne habilitée à les recevoir;

i) réexaminer à intervalles réguliers les listes de distribution et les destinataires habilités.

Informations supplémentaires

Ces procédures s'appliquent aux informations contenues dans les documents, les systèmes informatiques, les réseaux, les appareils informatiques mobiles, les communications mobiles, la messagerie électronique, la messagerie vocale, toute télécommunication en général où la voix est transmise, le multimédia, les services/équipements postaux, l'utilisation de télécopieurs et de toute autre pièce sensible comme des chèques en blanc ou des factures.

10.7.4 Sécurité de la documentation système

Mesure

Il convient de protéger la documentation système contre les accès non autorisés.

Préconisations de mise en œuvre

Pour sécuriser la documentation système, il convient de prendre en compte les éléments suivants:

a) il convient de stocker la documentation système de façon sécurisée;

b) il convient que le propriétaire de l'application réduise le plus possible la liste des personnes ayant accès à la documentation système;

c) il convient de protéger de façon adéquate la documentation système stockée sur un réseau public ou fournie via un réseau public.

Informations supplémentaires

La documentation système peut contenir une gamme d'informations sensibles, comme des descriptifs de processus applicatifs, des procédures, des structures de données ou des processus d'habilitation.

10.8 Échange des informations

Objectif: maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure.

Il convient de fonder les échanges d'informations et de logiciels entre organismes sur une politique d'échange formelle, élaborée conformément aux accords sur les échanges et il convient que ces échanges d'informations soient compatibles avec la législation applicable (voir Article 15).

Il convient d'élaborer des procédures et des normes pour protéger les informations et les supports physiques contenant des informations en transit.

10.8.1 Politiques et procédures d'échange des informations

Mesure

Il convient de mettre en place des politiques, procédures et mesures d'échange formelles pour protéger les échanges d'informations transitant par tous types d'équipements de télécommunication.

Préconisations de mise en œuvre

Il convient que les procédures et mesures à suivre pour les équipements de communication électronique servant aux échanges d'informations prennent en compte les points suivants:

a) les procédures conçues pour protéger les informations échangées contre l'interception, la reproduction, la modification, les erreurs d'acheminement et la destruction;

b) les procédures pour la détection et la protection contre les codes malveillants qui peut être transmis via les communications électroniques (voir 10.4.1);

c) les procédures pour protéger les informations sensibles communiquées électroniquement sous forme de pièces jointes;

d) une politique ou des directives décrivant succinctement l'utilisation acceptable des équipements de communication électronique (voir 7.1.3);

e) des procédures pour utiliser les communications sans fil en tenant compte des risques particuliers associés;

f) les salariés, les contractants ou toute autre utilisateur ne doivent pas compromette l'organisme, par exemple par diffamation, harcèlement, usurpation d'identité, renvoi de chaînes de messages, achats non autorisés, etc.;

g) l'utilisation de techniques de cryptographie, par exemple pour protéger la confidentialité, l'intégrité et l'authenticité de l'information (voir 12.3).

h) les directives sur la conservation et la mise au rebut de toutes les correspondances commerciales, dont les messages, conformément aux législations et réglementations nationales et locales applicables;

i) ne pas laisser d'informations sensibles ou critiques sur les équipements d'impression, comme les photocopieuses, les imprimantes et les télécopieurs, étant donné qu'ils sont accessibles au personnel non habilité;

j) les mesures et les restrictions liées au renvoi de messages par les équipements de télécommunication, comme le renvoi automatique de courriers électroniques vers des adresses électroniques extérieures;

k) rappeler au personnel qu'il convient de prendre les précautions appropriées, par exemple ne pas révéler d'informations sensibles au téléphone car elles risqueraient d'être entendues ou interceptées par

   1) les personnes du voisinage immédiat, en particulier lors de l'utilisation d'un téléphone mobile,

   2) la pose de micros sur le téléphone et autres formes de mise sur écoute, soit par accès physique au combiné ou à la ligne téléphonique, soit au moyen de scanners,

   3) les personnes dans le voisinage de l'interlocuteur;

l) ne pas laisser de messages comportant des informations sensibles sur les répondeurs puisque ces derniers peuvent être réécoutés par des personnes non habilitées, stockés sur des systèmes à usage collectif ou incorrectement mémorisés à la suite d'une erreur de numérotation;

m) rappeler au personnel les problèmes qu'entraîne l'utilisation de télécopieurs, à savoir:

   1) l'accès non autorisé aux mémoires des messages intégrées pour récupérer des messages;

   2) la programmation délibérée ou accidentelle de machines pour qu'elles envoient des messages à des numéros précis;

   3) l'envoi de documents et de messages au mauvais numéro soit par erreur de numérotation, soit par utilisation d'un mauvais numéro mémorisé;

n) rappeler au personnel de ne pas renseigner de données démographiques, comme l'adresse électronique ou autres informations personnelles, dans aucun logiciel pour éviter qu'elles ne soient recueillies à des fins non autorisées;

o) rappeler au personnel que les télécopieurs et les photocopieurs actuels comportent des mémoires cache qui stockent les pages; en cas de panne de papier ou de transmission, ces pages s'impriment une fois la panne éliminée.

En outre, il convient de rappeler au personnel qu'il est recommandé de pas avoir de conversation confidentielle dans des lieux publics, les bureaux ouverts ou des lieux de réunion dont les murs ne sont pas insonorisés.

Il convient que les équipements d'échange des informations soient conformes aux exigences légales applicables (voir Article 15).

Informations supplémentaires

L'échange d'informations peut se produire par le biais de nombreux types d'équipements de télécommunication différents, dont la messagerie électronique, la voix, le fax et la vidéo.

L'échange de logiciels peut se produire par des moyens nombreux et variés, notamment les téléchargements depuis Internet et l'acquisition auprès d'éditeurs fournissant des logiciels clé en main.

Dans l'échange de données électroniques, le commerce électronique et les communications électroniques, il convient de prendre en compte les implications pour l'activité, pour la sécurité et au regard du droit, ainsi que les exigences en termes de contrôles.

Les informations pourraient être compromises par le manque de sensibilisation des utilisateurs, de politiques ou de procédures sur l'utilisation des équipements d'échange des informations, par exemple si une personne entend dans un lieu public votre conversation au téléphone mobile, par accès non autorisé aux systèmes de consultation à distance de la messagerie vocale, ou par envoi accidentel de télécopies au mauvais télécopieur.

L'exploitation de l'activité pourrait être perturbée et l'information compromise en cas de panne, de surcharge ou d'interruption des équipements de télécommunications (voir 10.3 et Article 14). Les informations pourraient être compromises par l'accès d'utilisateurs non habilités (voir Article 11).

10.8.2 Accords d'échange

Mesure

Il convient de conclure des accords pour l'échange d'informations et de logiciels entre l'organisme et la partie externe.

Préconisations de mise en œuvre

Il convient que les accords d'échange prennent en compte les conditions de sécurité suivantes:

a) des responsabilités de gestion pour contrôler et informer de la transmission, de la répartition et de la réception;

b) des procédures pour informer l'expéditeur de la transmission, de la répartition et de la réception;

c) des procédures pour assurer la traçabilité et le non-répudiation;

d) des normes techniques minimales pour l'encapsulation et la transmission;

e) des accords de séquestre;

f) des normes d'identification du coursier;

g) les utilisateurs en charge et la responsabilité juridique en cas d'incident lié à la sécurité de l'information, comme la perte de données;

h) l'utilisation convenue d'un système de marquage pour les informations sensibles ou critiques permettant d'assurer la compréhension immédiate des étiquettes et la protection appropriée des informations;

i) la propriété et les responsabilités pour la protection des données, le copyright, la conformité à la licence logicielle et autres considérations semblables (voir 15.1.2 et 15.1.4);

j) les normes techniques pour l'enregistrement et la lecture des informations et des logiciels;

k) toute mesure particulière qui peut être nécessaire pour protéger des pièces sensibles, comme l'utilisation de clés cryptographiques (voir 12.3).

Il convient d'établir et de tenir à jour des politiques, procédures et normes pour protéger les informations et les supports physiques en transit (voir également 10.8.3), et il convient de les mentionner dans les accords d'échange.

Il convient que la partie sécurité de tout accord reflète la sensibilité des informations liées à l'activité qui sont en jeu.

Informations supplémentaires

Les accords peuvent être conclus de façon électronique ou manuelle et peuvent prendre la forme de contrats formels ou de conditions de louage de travail. Pour les informations sensibles, il convient que les mécanismes spécifiques employés pour échanger lesdites informations soient homogènes dans tous les organismes et pour tous les types d'accords.

10.8.3 Supports physiques en transit

Mesure

Il convient de protéger les supports contenant des informations contre les accès non autorisés, le mauvais usage ou l'altération lors du transport hors des limites physiques de l'organisme.

Préconisations de mise en œuvre

Pour le transport des supports d'informations entre plusieurs sites, il convient de prendre en compte les directives suivantes:

a) il convient que le transporteur ou le coursier utilisé soit fiable;

b) il convient de convenir de la liste des coursiers habilités avec la direction;

c) il convient de mettre au point des procédures pour contrôler l'identification des coursiers;

d) il convient que l'emballage choisi soit suffisant pour protéger son contenu de tout dommage physique susceptible de survenir lors du transit et qu'il soit conforme aux spécifications du fabricant (par exemple pour les logiciels), en servant par exemple de protection contre tout facteur environnemental pouvant diminuer l'efficacité de la restauration du support, comme l'exposition à de fortes températures, à une forte humidité ou aux champs électromagnétiques;

e) il convient, le cas échéant, d'adopter des mesures pour protéger les informations sensibles d'une divulgation ou d'une modification non autorisée; voici des exemples de ces mesures:

   1) l'utilisation de contenants fermant à clé;

   2) la livraison en main propre;

   3) un emballage inviolable (permettant de repérer facilement toute tentative d'effraction);

4) dans des cas exceptionnels, scinder l'expédition en plusieurs livraisons et la répartir sur différents itinéraires.

Informations supplémentaires

Les informations peuvent être vulnérables à un accès non autorisé, à un mauvais usage ou à une altération pendant le transport physique, par exemple lors de l'envoi de supports par courrier ou par coursier.

10.8.4 Messagerie électronique

Mesure

Il convient de protéger de manière adéquate les informations transitant par la messagerie électronique.

Préconisations de mise en œuvre

Pour la sécurité de la messagerie électronique, il convient de prendre en compte ce qui suit:

a) la protection des messages contre l'accès non autorisé, la modification ou le refus de service;

b) la qualité de l'adressage et du transport du message;

c) la disponibilité et la fiabilité générales du service;

d) les questions juridiques, comme les exigences en matières de signatures numériques;

e) l'obtention d'un accord avant d'utiliser des services externes publics comme la messagerie instantanée ou le partage de fichiers;

f) des niveaux plus élevés d'authentification permettant de contrôler l'accès depuis les réseaux accessibles au public.

Informations supplémentaires

La messagerie électronique comme les courriers électroniques, l'échange de données informatisé (EDI) et la messagerie instantanée jouent un rôle important dans les communications professionnelles. La messagerie électronique comporte des risques différents de la communication papier.

10.8.5 Systèmes d'information d'entreprise

Mesure

Il convient d'élaborer et de mettre en œuvre des politiques et procédures pour protéger l'information liée à l'interconnexion de systèmes d'informations d'entreprise.

Préconisations de mise en œuvre

Parmi les implications de l'interconnexion de ces équipements pour la sécurité et l'activité, il convient de prendre en compte les éléments suivants:

a) les vulnérabilités connues dans les systèmes d'administration et de comptabilité dans lesquels l'information est partagée entre diverses parties de l'organisme;

b) les vulnérabilités de l'information dans les systèmes de télécommunication d'entreprise, comme l'enregistrement des appels téléphoniques à deux ou en conférence, la confidentialité des appels, le stockage des fax, l'ouverture et la distribution du courrier;

c) la politique et les mesures adéquates pour gérer le partage de l'information;

d) des catégories d'exclusion d'informations sensibles liées à l'activité et de documents classés lorsque le système ne fournit pas le niveau de protection approprié (voir 7.2);

e) la restriction de l'accès aux informations quotidiennes relatives à des personnes sélectionnées, par exemple le personnel qui travaille sur des projets sensibles;

f) les catégories de personnel, contractants ou partenaires commerciaux autorisés à utiliser le système et les emplacements depuis lesquels ils peuvent y accéder (voir 6.2 et 6.3);

g) la restriction d'équipements sélectionnés à des catégories précises d'utilisateurs;

h) l'identification du statut des utilisateurs dans les répertoires de l'organisme, par exemple salarié ou contractant, dans l'intérêt des autres utilisateurs;

i) la conservation et la sauvegarde d'informations stockées sur le système (voir 10.5.1);

j) les exigences et les dispositions de repli (voir Article 14).

Informations supplémentaires

Au bureau, les systèmes d'informations permettent de disséminer et partager plus rapidement l'information en combinant: les documents, les ordinateurs, les appareils informatiques mobiles, les communications mobiles, la messagerie électronique, la messagerie vocale, toute télécommunication en général où la voix est transmise, le multimédia, les services/équipements postaux ou les télécopieurs.

10.9 Services de commerce électronique

Objectif: assurer la sécurité des services de commerce électronique, tout comme leur utilisation sécurisée.

Il convient de prendre en compte les implications pour la sécurité de l'utilisation de services de commerce électronique, comme les transactions en ligne, ainsi que les exigences en matière de contrôles. Il convient de prendre également en compte l'intégrité et la disponibilité des informations publiées sous format électronique au travers de systèmes accessibles au public.

10.9.1 Commerce électronique

Mesure

Il convient de protéger l'information transitant par le commerce électronique transmise sur les réseaux publics contre les activités frauduleuses, les litiges sur les contrats et la divulgation et la modification non autorisées.

Préconisations de mise en œuvre

Pour la sécurité du commerce électronique, il convient de prendre en compte ce qui suit:

a) le niveau de confiance que chaque partie requiert sur l'identité déclarée des autres au moyen, par exemple, de l'authentification;

b) les processus d'autorisation pour qui peut fixer les prix, émettre ou signer des documents commerciaux;

c) s'assurer que les partenaires commerciaux sont pleinement informés de leurs autorisations;

d) déterminer et satisfaire les exigences en matière de confidentialité, d'intégrité, de preuve de la répartition et de la réception des documents-clés et de non-répudiation des contrats, dans le contexte par exemple d'appels d'offre et contrats;

e) le niveau de confiance requis pour l'intégrité des tarifs publiés;

f) la confidentialité de toute donnée ou information sensible;

g) la confidentialité et l'intégrité de toutes transactions de commandes, de détails de paiement, de coordonnées de livraison et de confirmation de réception;

h) le degré de vérification adéquat pour contrôler les détails de paiement fournis par le client;

i) sélectionner le mode de règlement le plus adapté pour se prémunir de la fraude;

j) le niveau de protection requis pour maintenir la confidentialité et l'intégrité des éléments du bon de commande;

k) éviter la perte ou la duplication des détails de la transaction;

l) la responsabilité juridique induite par toute transaction frauduleuse;

m) les exigences de l'assureur.

Nombreuses sont les considérations ci-dessus qui peuvent être satisfaites par l'application de mesures de cryptographie (voir 12.3) qui tiennent compte de la conformité avec les exigences légales (voir 15.1 et plus particulièrement 15.1.6 pour la législation en matière de cryptographie).

Il convient de mettre à l'appui des dispositions sur le commerce électronique entre partenaires commerciaux un accord documenté qui engage les deux parties aux conditions commerciales convenues, parmi lesquelles les détails de l'autorisation [voir le point b) ci-dessus]. D'autres accords conclus avec les fournisseurs de réseau à valeur ajoutée et de services d'information peuvent être nécessaires.

Il convient pour les systèmes de commerce en ligne de publier leurs conditions de vente aux clients.

Il convient de tenir compte de la résistance des hôtes aux attaques pratiquées dans le commerce électronique et des implications pour la sécurité que représente toute interconnexion de réseaux requise pour la mise en œuvre de services de commerce électronique (voir 11.4.6).

Informations supplémentaires

Le commerce électronique est vulnérable à de nombreuses menaces pour le réseau pouvant résulter d'activités frauduleuses, de litiges sur les contrats et de divulgation et modification non autorisées de l'information.

Le commerce électronique peut employer des méthodes d'authentification sécurisée pour réduire les risques, par exemple grâce à la cryptographie à clé publique et aux signatures numériques (voir également 12.3). Des services tiers de confiance peuvent également être utilisés, le cas échéant.

10.9.2 Transactions en ligne

Mesure

Il convient de protéger les informations transitant par les transactions en ligne pour empêcher la transmission incomplète, les erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou la réémission.

Préconisations de mise en œuvre

Pour la sécurité des transactions en ligne, il convient de prendre en compte les éléments suivants:

a) l'utilisation de signatures électroniques par chacune des parties impliquées dans la transaction;

b) l'ensemble des aspects de la transaction, ce qui revient à s'assurer que

   1) les références utilisateur de toutes les parties sont valables et ont fait l'objet d'une vérification,

2) la transaction demeure confidentielle, et que

3) le respect de la vie privée de toutes les parties impliquées est maintenu;

c) le canal de communication entre toutes les parties impliquées est chiffré;

d) les protocoles utilisés pour la communication entre les parties sont sécurisés;

e) veiller à ce que le stockage des détails de la transaction soit situé hors de tout environnement accessible au public, à l'instar d'une plate-forme de stockage en place sur l'intranet de l'organisme, et qu'il ne soit pas conservé ou exposé sur un support de stockage directement accessible depuis Internet;

f) lorsqu'une autorité de confiance est utilisée (aux fins d'émettre et de tenir à jour des signatures et/ou certificats électroniques), la sécurité est intégrée et imbriquée tout au long du processus de gestion de bout en bout des certificats ou signatures.

Informations supplémentaires

Il sera nécessaire que l'étendue des mesures adoptées soit fonction du niveau de risque associé à chaque type de transaction en ligne.

Les transactions peuvent nécessiter une conformité avec les lois, règlements et réglementation en vigueur dans la juridiction dans laquelle elles sont générées, traitées ou achevées et/ou stockées.

Il existe plusieurs types de transactions qui peuvent être effectuées en ligne, comme les transactions contractuelles, financières, etc.

10.9.3 Informations à disposition du public

Mesure

Il convient de protéger l'intégrité des informations mises à disposition sur un système accessible au public pour empêcher toute modification non autorisée.

Préconisations de mise en œuvre

Il convient de protéger par des mécanismes adéquats, comme les signatures électroniques (voir 12.3), les logiciels, données et autres informations nécessitant un haut niveau d'intégrité, qui sont mis à disposition sur un système accessible au public. Il convient de soumettre à essai les systèmes accessibles au public afin de détecter les failles et les pannes éventuelles avant la mise à disposition de l'information.

Il convient de suivre un processus d'accord formel avant de mettre l'information à disposition du public. En outre, il convient que toutes les données saisies qui sont extérieures au système soient vérifiées et validées.

Il convient de contrôler soigneusement les systèmes de publication électronique, en particulier ceux qui permettent de laisser ses impressions et de saisir des informations directement, de sorte que

a) l'information soit obtenue en conformité avec toute législation en matière de protection des données (voir 15.1.4),

b) l'information saisie dans et traitée par le système de publication soit traitée complètement, avec exactitude et en temps voulu,

c) les informations sensibles soient protégées lors de leur collecte, de leur traitement et de leur stockage, et

d) l'accès au système de publication n'autorise pas d'accès involontaire aux réseaux auxquels le système est connecté.

Informations supplémentaires

Les informations stockées sur un système accessible au public, comme les informations sur un serveur web qui sont accessibles via Internet, peuvent nécessiter de satisfaire aux lois, règlements et réglementations en vigueur dans la juridiction où le système est situé, où l'échange commercial a lieu ou encore où le(s) propriétaire(s) réside. La modification non autorisée d'informations publiées peut nuire à la réputation de l'organisme responsable de leur publication.

10.10 Surveillance

Objectif: détecter les traitements non autorisés de l'information.

Il convient de mettre en place une surveillance des systèmes et d'enregistrer les événements liés à la sécurité de l'information. Il convient d'utiliser un journal des opérations et des rapports de défaut pour garantir la détection des problèmes liés au système d'information.

Il convient qu'un organisme soit en conformité avec toutes les exigences légales applicables à ses activités de surveillance et de journalisation des événements.

Il convient d'utiliser la surveillance du système pour vérifier l'efficacité des mesures adoptées et pour vérifier la conformité avec le protocole d'accès.

10.10.1 Rapport d'audit

Mesure

Il convient que les rapports d'audit, qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité soient produits et conservés pendant une période préalablement définie afin de faciliter les investigations ultérieures et la surveillance du contrôle d'accès.

Préconisations de mise en œuvre

Il convient que les rapports d'audit contiennent les informations suivantes, s'il y a lieu:

a) les identifiants utilisateurs;

b) la date, l'heure et les détails relatifs aux événements significatifs, par exemple les ouvertures et fermetures de session;

c) l'identification du terminal ou son emplacement, si possible;

d) les enregistrements des tentatives d'accès au système, réussies et avortées;

e) les enregistrements des tentatives d'accès aux données et autres ressources, qu'elles soient réussies ou avortées;

f) les modifications apportées à la configuration du système;

g) l'utilisation des privilèges;

h) l'emploi des utilitaires et des applications;

i) les fichiers qui ont fait l'objet d'un accès et la nature de l'accès;

j) les adresses et les protocoles du réseau;

k) les alarmes déclenchées par le système de contrôle d'accès;

l) l'activation et la désactivation des systèmes de protection, tels que les systèmes antivirus et les systèmes de détection des intrusions.

Informations supplémentaires

Les rapports d'audit peuvent contenir des données personnelles confidentielles ou soumises au droit des libertés individuelles. Il convient de prendre des mesures appropriées visant à protéger la vie privée (voir également 15.1.4). Lorsque cela est possible, il convient que les administrateurs systèmes ne soient pas habilités à effacer les rapports concernant leurs propres activités ou à désactiver l'historisation de ces activités (voir 10.1.3).

10.10.2 Surveillance de l'exploitation du système

Mesure

Il convient d'établir des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information et de réexaminer périodiquement les résultats des activités de surveillance.

Préconisations de mise en œuvre

Il convient de déterminer le niveau de surveillance requis pour chaque équipement par le biais d'une appréciation du risque. Il convient qu'un organisme soit en conformité avec toutes les exigences légales applicables à ses activités de surveillance. Les domaines concernés sont les suivants:

a) l'accès autorisé, notamment les éléments suivants:

   1) l'identifiant utilisateur;

   2) la date et l'heure des événements clé;

   3) les types d'événements;

   4) les fichiers qui ont été consultés;

   5) le programme/les utilitaires utilisé(s);

b) toutes les opérations nécessitant des privilèges, par exemple:

   1) l'utilisation de comptes dotés de privilèges, par exemple, superviseur, racine, administrateur;

   2) le démarrage et l'arrêt du système;

   3) la connexion ou la déconnexion de périphériques d'entrée/sortie;

c) les tentatives d'accès non autorisées, par exemple:

   1) les opérations utilisateurs refusées ou ayant débouché sur un échec;

   2) les opérations utilisateurs concernant des données ou d'autres ressources ayant entraîné un refus ou un échec;

   3) les violations de la politique d'accès et les notifications relatives aux passerelles réseau et aux pare-feu;

   4) les alarmes émises par les systèmes propriétaires de détection des intrusions;

d) les alarmes système ou les défaillances, par exemple:

   1) les alarmes ou les messages émis par les consoles;

   2) les journaux système d'événements exceptionnels;

3) les alarmes liées à la gestion du réseau;

4) les alarmes déclenchées par le système de contrôle d'accès;

e) les modifications ou tentatives de modification des paramètres et des mesures de sécurité du système.

Il convient de définir la fréquence à laquelle les résultats des activités de surveillance sont revus en fonction des risques. Il convient d'envisager les facteurs de risque suivants:

a) criticité des processus de l'application;

b) valeur, sensibilité et criticité des informations concernées;

c) expérience acquise en matière d'intrusion et de mauvais usage, ainsi que la fréquence à laquelle les vulnérabilités sont exploitées;

d) ampleur de l'interconnexion système (en particulier les réseaux publics);

e) équipements de journalisation désactivés.

Informations supplémentaires

Des procédures de surveillance sont nécessaires pour s'assurer que les opérations réalisées par les utilisateurs sont explicitement autorisées.

Un réexamen des rapports consiste à analyser les menaces auxquelles le système est exposé et à déterminer leur mode d'apparition. Des exemples d'événements susceptibles de nécessiter un complément d'investigation en cas d'incidents liés à la sécurité de l'information sont présentés en 13.1.1.

10.10.3 Protection des informations journalisées

Mesure

Il convient de protéger les équipements de journalisation et les informations journalisées contre le sabotage et les accès non autorisés.

Préconisations de mise en œuvre

Il convient que les mesures soient conçues pour assurer une protection de l'équipement de journalisation contre les modifications non autorisées et les dysfonctionnements, à savoir:

a) la modification des types de message enregistrés;

b) la modification ou la suppression des fichiers journaux;

c) le dépassement de la capacité de stockage du fichier journal, qui a pour effet d'empêcher l'enregistrement des événements ou d'écraser les événements déjà enregistrés.

Il peut être nécessaire d'archiver certains rapports d'audit dans le cadre de la politique de conservation des enregistrements ou à des fins de collecte et de conservation de preuves (voir également 13.2.3).

Informations supplémentaires

Les journaux système contiennent souvent un gros volume d'informations. La plupart de ces informations ne concernent pas la surveillance liée à la sécurité. Pour faciliter la détection des événements significatifs dans le cadre de la surveillance liée à la sécurité, il convient d'envisager la copie automatique des types de messages dans un second journal et/ou d'utiliser les utilitaires système ou les outils d'audit appropriés pour interroger et rationaliser les fichiers.

Il est nécessaire de protéger les journaux système, car s'il est possible de modifier ou d'effacer les données qu'ils contiennent, leur existence peut créer une fausse impression de sécurité.

10.10.4 Journal administrateur et journal des opérations

Mesure

Il convient de journaliser les activités de l'administrateur système et de l'opérateur système.

Préconisations de mise en œuvre

Il convient que les journaux incluent les éléments suivants:

a) l'heure à laquelle un événement est survenu (succès ou échec);

b) les informations relatives à l'événement (par exemple les fichiers concernés) ou à la défaillance (par exemple l'erreur et l'action corrective correspondante);

c) l'identification du compte et de l'administrateur ou de l'opérateur concerné;

d) les processus concernés.

Il convient que le journal administrateur et le journal des opérations système soient périodiquement soumis à un réexamen.

Informations supplémentaires

Pour vérifier la conformité des activités d'administration système et réseau, il est possible d'utiliser un système de détection d'intrusion hors du contrôle des administrateurs système et réseau.

10.10.5 Rapports de défaut

Mesure

Il convient de journaliser et d'analyser les éventuels défauts et de prendre les mesures appropriées.

Préconisations de mise en œuvre

Il convient de journaliser les défauts signalés par les utilisateurs ou les programmes au niveau des systèmes de traitement de l'information ou de communication. Il convient de définir des règles claires pour traiter les défauts signalés, notamment:

a) un réexamen des rapports de défaut, afin de garantir la bonne correction des défauts;

b) un réexamen des actions correctives, afin de vérifier que les mesures n'ont pas été compromises et que l'opération est pleinement autorisée.

Si le système comporte un journal des erreurs, il convient de s'assurer que cette fonction est activée.

Informations supplémentaires

La journalisation des erreurs et des défauts peut avoir une incidence sur les performances d'un système. Il convient que cette fonction soit activée par le personnel compétent et que le niveau de journalisation requis pour chaque système soit déterminé par le biais d'une appréciation du risque, en tenant compte de la dégradation des performances.

10.10.6 Synchronisation des horloges

Mesure

Il convient de synchroniser les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité à l'aide d'une source de temps précise et préalablement définie.

Préconisations de mise en œuvre

Lorsqu'un ordinateur ou un dispositif de communication a la capacité de commander une horloge en temps réel, il convient d'étalonner cette horloge sur une référence reconnue, par exemple le temps universel coordonné (UTC) ou l'heure locale. Certaines horloges dérivent avec le temps. Il convient par conséquent de définir une procédure permettant de vérifier l'absence de variations significatives et de corriger les éventuelles variations.

La bonne interprétation du format date/heure est essentielle pour garantir la conformité de l'horodatage avec la date et l'heure réelles. Il convient de tenir compte des spécificités locales (par exemple les changements d'heure visant à économiser l'électricité).

Informations supplémentaires

Le bon paramétrage des horloges est important, car il influe sur la précision des rapports d'audit qui peuvent être utilisés lors d'investigations ou servir de preuves en cas de litige ou de sanction disciplinaire. Des rapports d'audit imprécis peuvent gêner les investigations et porter atteinte à la crédibilité des preuves. Pour les systèmes de journalisation, il est possible d'utiliser une horloge maître reliée à un signal horaire radiodiffusé par une horloge atomique nationale. Un protocole de synchronisation du réseau peut être utilisé pour garantir la synchronisation de tous les serveurs avec l'horloge maître.

11 Contrôle d'accès

11.1 Exigences métier relatives au contrôle d'accès

Objectif: maîtriser l'accès à l'information.

Il convient que l'accès à l'information, aux moyens de traitement de l'information et aux processus métier soit contrôlé sur la base des exigences d'exploitation et de sécurité.

Il convient que les règles de contrôle d'accès tiennent compte des politiques de diffusion de l'information et d'autorisation.

11.1.1 Politique de contrôle d'accès

Mesure

Il convient d'établir, de documenter et de réexaminer une politique de contrôle d'accès sur la base des exigences d'exploitation et de sécurité.

Préconisations de mise en œuvre

Il convient de formuler de manière claire les règles et les droits en matière de contrôle d'accès pour chaque utilisateur ou groupe d'utilisateurs dans le cadre d'une politique de contrôle d'accès. Les contrôles d'accès sont à la fois logiques et physiques (voir également Article 9) et il est bon de les envisager conjointement. Il convient que les utilisateurs et les prestataires de services soient clairement informés des exigences métier qui sont à l'origine des contrôles d'accès.

Il convient que la politique tienne compte des exigences suivantes:

a) exigences en matière de sécurité pour chaque application de gestion;

b) identification de toutes les informations liées aux applications de gestion et des risques auxquels l'information est exposée;

c) politiques relatives à la diffusion de l'information et aux autorisations, par exemple nécessité de connaître le principe, les niveaux de sécurité et la classification des informations (voir 7.2);

d) cohérence entre la politique de contrôle d'accès et la politique de classification des informations pour différents systèmes et réseaux;

e) législation et obligations contractuelles applicables relatives à la protection de l'accès aux données ou aux services (voir 15.1);

f) profils d'accès utilisateur normalisés pour les rôles courants au sein de l'organisme;

g) gestion des droits d'accès dans un environnement distribué mis en réseau qui reconnaît tous les types de connexions disponibles;

h) cloisonnement des rôles pour le contrôle d'accès, par exemple la demande d'accès, l'autorisation d'accès et l'administration d'accès;

i) exigences en matière d'autorisation formelle des requêtes d'accès (voir 11.2.1);

j) exigences relatives à la fréquence de réexamen des contrôles d'accès (voir 11.2.4);

k) annulation de droits d'accès (voir 8.3.3).

Informations supplémentaires

Il convient de faire preuve de prudence lors de la spécification des règles de contrôle d'accès:

a) distinguer les règles qui doivent être toujours appliquées et les lignes directrices qui sont optionnelles ou conditionnelles;

b) établir des règles fondées sur le principe suivant: «tout est généralement interdit sauf autorisation expresse» plutôt que sur la règle, moins fiable, selon laquelle «tout est généralement autorisé sauf interdiction expresse»;

c) considérer les modifications apportées automatiquement aux étiquettes (voir 7.2) par les moyens de traitement de l'information, et les modifications qui sont à l'appréciation de l'utilisateur;

d) considérer les modifications apportées automatiquement aux droits d'accès de l'utilisateur par le système d'information, et les modifications qui sont décidées par un administrateur;

e) considérer les règles qui nécessitent une approbation spécifique avant toute mise en œuvre, et les règles pour lesquelles aucune autorisation préalable n'est nécessaire.

Il convient que les règles de contrôle d'accès s'appuient sur des procédures formelles et des responsabilités clairement définies (voir par exemple 6.1.3, 11.3, 10.4.1 et 11.6).

11.2 Gestion de l'accès utilisateur

Objectif: maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes d'information.

Il convient de mettre en place des procédures formelles pour contrôler l'attribution de droits d'accès aux systèmes et services d'information.

Il convient que ces procédures couvrent toutes les étapes du cycle de vie de l'accès utilisateur, depuis l'enregistrement initial des nouveaux utilisateurs jusqu'à la désinscription des utilisateurs pour lesquels l'accès aux systèmes et services d'information est devenu inutile. Il convient d'accorder une attention particulière, le cas échéant, à la nécessité de maîtriser l'attribution de privilèges en termes de droits d'accès, qui permet aux utilisateurs de contourner les mesures système.

11.2.1 Enregistrement des utilisateurs

Mesure

Il convient de définir une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information.

Préconisations de mise en œuvre

Il convient que la procédure de contrôle d'accès pour l'enregistrement et la désinscription des utilisateurs comprenne les actions suivantes:

a) créer des identifiants utilisateurs uniques permettant d'identifier les utilisateurs sans ambiguïté et de les responsabiliser; il convient d'autoriser l'utilisation de groupes d'identifiants uniquement lorsque les aspects opérationnels et liés à l'activité de l'organisme l'exigent; il convient que ces groupes soient approuvés et documentés;

b) vérifier que le propriétaire du système a habilité l'utilisateur à accéder au système ou au service d'information; une approbation séparée de la direction concernant les droits d'accès peut également être appropriée;

c) vérifier que le niveau d'accès accordé est adapté à la finalité fonctionnelle (voir 11.1) et conforme à la politique de sécurité de l'organisme; vérifier par exemple qu'il ne met pas en péril la séparation des tâches (voir 10.1.3);

d) fournir aux utilisateurs une déclaration écrite concernant leurs droits d'accès;

e) faire signer aux utilisateurs une déclaration indiquant qu'ils comprennent les conditions d'accès;

f) veiller à ce que les prestataires de services n'accordent pas d'accès tant que le processus d'autorisation n'est pas terminé;

g) tenir à jour un enregistrement formel de toutes les personnes auxquelles un droit d'accès a été attribué pour le service en question;

h) supprimer ou bloquer immédiatement les droits d'accès des utilisateurs qui ont changé de rôle ou de fonction ou qui ont quitté l'organisme;

i) vérifier périodiquement et éventuellement supprimer ou bloquer les identifiants et les comptes utilisateurs redondants (voir 11.2.4);

j) veiller à ce que les identifiants utilisateurs redondants ne soient pas attribués à d'autres utilisateurs.

Informations supplémentaires

Il convient d'envisager d'établir des rôles d'accès utilisateurs sur la base des exigences métier, qui regroupent des droits d'accès dans des profils utilisateurs types. Les requêtes et les réexamens d'accès (voir 11.2.4) sont plus faciles à gérer au niveau de ce type de rôles qu'au niveau des droits d'accès individuels.

Il convient d'envisager d'inclure des clauses dans les contrats de travail et les contrats de service stipulant les sanctions encourues en cas de tentative d'accès non autorisé par un salarié ou un prestataire de service (voir également 6.1.5, 8.1.3 et 8.2.3).

11.2.2 Gestion des privilèges

Mesure

Il convient de restreindre et de contrôler l'attribution et l'utilisation des privilèges.

Préconisations de mise en œuvre

Pour les systèmes multi-utilisateurs nécessitant une protection contre les accès non autorisés, il convient de contrôler l'attribution des privilèges par le biais d'une procédure formelle d'autorisation. Il convient d'envisager les étapes suivantes:

a) il convient d'identifier les privilèges d'accès associés à chaque produit système, par exemple le système d'exploitation, le système de gestion de la base de données et chaque application, ainsi que les utilisateurs auxquels il est nécessaire d'attribuer ces privilèges;

b) il convient d'attribuer des privilèges aux utilisateurs suivant les impératifs liés à leur activité ou au cas par cas, en conformité avec la politique de contrôle d'accès (11.1.1), c'est-à-dire les exigences minimales pour leur rôle fonctionnel, seulement si nécessaire;

c) il convient de tenir à jour une procédure d'autorisation et un enregistrement de tous les privilèges qui ont été attribués. Il convient de ne pas attribuer des privilèges tant que le processus d'autorisation n'est pas terminé;

d) il convient de favoriser la mise au point et l'utilisation de routines système afin d'éviter l'attribution de privilèges utilisateurs;

e) il convient également d'encourager la mise au point et l'utilisation de programmes permettant d'éviter de recourir à des privilèges;

f) il convient d'associer les privilèges à un identifiant utilisateur différent des identifiants utilisés dans le cadre des activités de gestion courantes.

Informations supplémentaires

Une mauvaise utilisation des privilèges d'administration (toute fonction ou tout équipement d'un système d'information permettant de contourner les mesures système ou applicatives) peut constituer une source importante de défaillance ou de vulnérabilité dans les systèmes.

11.2.3 Gestion du mot de passe utilisateur

Mesure

Il convient que l'attribution de mots de passe soit réalisée dans le cadre d'un processus formel.

Préconisations de mise en œuvre

Il convient que ce processus prévoie les exigences suivantes:

a) il convient de faire signer aux utilisateurs une déclaration par laquelle ils s'engagent à ne pas divulguer leurs mots de passe personnels et à communiquer leurs mots de passe de groupe d'utilisateurs aux seuls utilisateurs du groupe; il est possible d'inclure cette déclaration signée dans le contrat de travail (voir 8.1.3);

b) lorsque les utilisateurs ont la responsabilité de gérer eux-mêmes leurs mots de passe, il convient de leur fournir initialement un mot de passe temporaire sécurisé (voir 11.3.1), qu'ils doivent changer immédiatement;

c) établir des procédures permettant de vérifier l'identité d'un utilisateur avant d'attribuer un nouveau mot de passe ou un mot de passe temporaire;

d) il convient que la communication des mots de passe utilisateurs temporaires soit sécurisée; il convient de ne pas utiliser un courrier électronique non protégé (texte en clair) ou appartenant à un tiers;

e) il convient que chaque mot de passe temporaire soit attribué à une personne unique et ne puisse pas être deviné;

f) il convient que les utilisateurs accusent réception de leurs mots de passe;

g) il convient que les mots de passe ne soient en aucune circonstance stockés sur un support informatique sous une forme non protégée;

h) il convient que les mots de passe par défaut définis par les constructeurs et éditeurs soient modifiés après installation des systèmes ou logiciels.

Informations supplémentaires

Les mots de passe constituent une méthode couramment utilisée pour vérifier l'identité d'un utilisateur avant d'accorder l'accès à un système ou un service d'information, conformément à la procédure d'autorisation. Le cas échéant, il convient d'envisager l'utilisation d'autres technologies permettant l'identification et l'authentification de l'utilisateur, telles que la biométrie (par exemple vérification des empreintes digitales ou vérification de signature) et les jetons cryptographiques (par exemple les cartes à puce).

11.2.4 Réexamen des droits d'accès utilisateurs

Mesure

Il convient que la direction revoie les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel.

Préconisations de mise en œuvre

Il convient que le réexamen des droits d'accès utilisateurs tienne compte des lignes directrices suivantes:

a) il convient de réexaminer les droits d'accès utilisateurs à intervalles réguliers, par exemple tous les 6 mois, et après tout changement tel qu'une promotion, une rétrogradation ou le départ d'un salarié (voir 11.2.1);

b) il convient de réexaminer et de réattribuer les droits d'accès utilisateurs en cas de changement de fonction au sein de l'organisme;

c) il convient de réexaminer les autorisations accordées pour les droits d'accès utilisateurs dotés de privilèges spéciaux (voir 11.2.2) à une plus grande fréquence, par exemple, tous les 3 mois;

d) il convient de vérifier l'attribution de privilèges à intervalles réguliers pour s'assurer qu'aucun privilège non autorisé n'a été accordé;

e) il convient de journaliser les modifications apportées aux comptes dotés de privilèges pour les besoins du réexamen périodique.

Informations supplémentaires

Il est nécessaire de réexaminer à intervalles réguliers les droits d'accès utilisateurs afin de conserver un contrôle sur l'accès aux données et aux services d'information.

11.3 Responsabilités utilisateurs

Objectif: empêcher les accès utilisateurs non habilités et la compromission ou le vol d'informations et de moyens de traitement de l'information.

La coopération des utilisateurs habilités est essentielle à la sécurité.

Il convient que les utilisateurs soient informés de leurs responsabilités concernant le maintien de contrôles d'accès efficaces, en particulier concernant l'utilisation de mots de passe et la sécurité du matériel.

Il convient de mettre en œuvre une politique «du bureau propre et de l'écran vide» afin de réduire le risque d'accès non autorisé ou d'endommagement des supports, papiers ou autres, et des moyens de traitement de l'information.

11.3.1 Utilisation du mot de passe

Mesure

Il convient de demander aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.

Préconisations de mise en œuvre

Il convient de recommander aux utilisateurs les précautions suivantes:

a) ne pas communiquer leur mot de passe;

b) ne pas conserver d'enregistrement de leur mot de passe (par exemple sur support papier, fichier électronique ou équipement portable), sauf si le support de stockage est sûr et si la méthode de stockage a été approuvée;

c) changer de mot de passe lorsqu'ils soupçonnent une compromission du système ou du mot de passe;

d) choisir un mot de passe de qualité, suffisamment long et

   1) facile à retenir,

   2) ne pouvant pas être rattaché à une information personnelle facile à deviner ou à obtenir, par exemple nom, numéro de téléphone, date d'anniversaire,

   3) non vulnérable à une attaque par dictionnaire (c'est-à-dire un mot de passe uniquement composé d'un mot figurant dans les dictionnaires), et

   4) qui n'est pas composé de caractères consécutifs identiques, totalement numériques ou totalement alphabétiques;

e) changer de mot de passe à intervalles réguliers ou après un certain nombre d'accès (pour les comptes dotés de privilèges, il convient de changer de mot de passe plus fréquemment) et ne pas réutiliser ou recycler d'anciens mots de passe;

f) changer le mot de passe temporaire à la première ouverture de session;

g) ne pas inclure le mot de passe dans un processus de connexion automatique, par exemple en l'intégrant dans une macrocommande ou en l'associant à une touche de fonction;

h) ne pas partager un mot de passe utilisateur individuel;

i) ne pas utiliser le même mot de passe pour les activités professionnelles et extraprofessionnelles.

Si les utilisateurs ont besoin d'accéder à plusieurs services, systèmes ou plates-formes et qu'il leur est demandé d'utiliser plusieurs mots de passe distincts, il convient qu'ils soient informés de la possibilité d'utiliser un mot de passe unique et de qualité [voir le point d) ci-avant] pour tous les services pour lesquels l'utilisateur est assuré qu'un niveau de protection raisonnable a été établi pour chaque service, système ou plate-forme.

Informations supplémentaires

Il est nécessaire d'accorder une attention particulière à la gestion du système d'assistance qui s'occupe des mots de passe perdus ou oubliés, car il constitue une cible privilégiée en cas d'attaque.

11.3.2 Matériel utilisateur laissé sans surveillance

Mesure

Il convient que les utilisateurs s'assurent que tout matériel laissé sans surveillance est doté d'un dispositif de protection approprié.

Préconisations de mise en œuvre

Il convient que tous les utilisateurs soient informés des exigences et des procédures de sécurité concernant les matériels laissés sans surveillance, ainsi que de leurs responsabilités liées à la mise en œuvre d'une telle protection. Il convient de recommander aux utilisateurs ce qui suit:

a) fermer les sessions actives lorsqu'ils ont terminé, sauf si les sessions peuvent être sécurisées par un mécanisme de verrouillage approprié, par exemple un économiseur d'écran protégé par un mot de passe;

b) se déconnecter des ordinateurs centraux, des serveurs et des PC lorsqu'une session est terminée (c'est-à-dire de ne pas se contenter d'éteindre le terminal ou l'écran);

c) protéger les PC ou les terminaux contre toute utilisation non autorisée par le biais d'une clé ou d'un dispositif équivalent tel qu'un mot de passe, lorsqu'ils ne sont pas utilisés (voir également 11.3.3).

Informations supplémentaires

Les matériels installés dans les zones utilisateurs, par exemple les postes de travail ou les serveurs de fichiers, peuvent nécessiter une protection spécifique contre les accès non autorisés lorsqu'ils sont laissés sans surveillance pendant des périodes prolongées.

11.3.3 Politique du bureau propre et de l'écran vide

Mesure

Il convient d'adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information.

Préconisations de mise en œuvre

Il convient que les politiques du bureau propre et de l'écran vide tiennent compte des classes d'information (voir 7.2), des exigences légales et contractuelles (voir 15.1) ainsi que des risques associés et de la culture de l'organisme. Il convient d'envisager les étapes suivantes:

a) lorsque les informations sensibles ou critiques liées à l'activité de l'organisme, par exemple sous format papier ou électronique, sont non utilisées, il convient de les mettre sous clé, de préférence dans un coffre-fort, une armoire ou tout autre meuble offrant un bon niveau de sécurité), notamment lorsque les locaux sont vides;

b) lorsqu'ils sont laissés sans surveillance, il convient que les ordinateurs et terminaux soient déconnectés ou protégés par un verrouillage de l'écran ou du clavier contrôlé par un mot de passe, un jeton ou un autre mécanisme d'authentification de l'utilisateur. Il convient également qu'ils soient protégés par des clés, des mots de passe ou d'autres mesures lorsqu'ils sont non utilisés;

c) il convient de protéger les points d'entrée et de sortie des courriers postaux ainsi que les télécopieurs laissés sans surveillance;

d) il convient d'empêcher l'utilisation non autorisée des photocopieurs et autres dispositifs de reproduction (par exemple les scanners ou les appareils de photo numériques);

e) il convient de retirer immédiatement des imprimantes les documents contenant des informations sensibles ou classées.

Informations supplémentaires

La mise en place d'une politique du bureau propre et de l'écran vide permet de réduire les risques d'accès non autorisés, de perte et d'endommagement de l'information pendant les heures de travail et en dehors des heures de travail. L'utilisation de coffres-forts ou d'autres moyens de stockage sécurisés peut également contribuer à la protection de l'information contre les sinistres tels qu'incendies, tremblements de terre, inondations ou explosions.

Envisager l'utilisation d'imprimantes dotées d'une fonction d'identification par numéro personnel, afin que seules les personnes ayant lancé l'impression puissent récupérer les documents imprimés et uniquement lorsqu'elles se trouvent devant l'imprimante.

11.4 Contrôle d'accès au réseau

Objectif: empêcher les accès non autorisés aux services disponibles sur le réseau.

Il convient de contrôler l'accès aux services à la fois en interne et en externe.

Il convient que l'accès utilisateur au réseau et aux services en réseau ne nuise pas à la sécurité des services. Pour ce faire, s'assurer des aspects suivants:

a) adéquation des interfaces entre le réseau de l'organisme et les autres réseaux privés et publics;

b) utilisation de mécanismes d'authentification appropriés pour les utilisateurs et le matériel;

c) mise en application du contrôle d'accès des utilisateurs aux services d'information.

11.4.1 Politique relative à l'utilisation des services en réseau

Mesure

Il convient que les utilisateurs aient uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.

Préconisations de mise en œuvre

Il convient de définir une politique relative à l'utilisation des réseaux et des services en réseau. Il convient que cette politique couvre les aspects suivants:

a) les réseaux et les services en réseau pour lesquels l'accès a été accordé;

b) les procédures d'autorisation désignant les personnes habilitées à accéder à tel ou tel réseau et service en réseau;

c) les procédures et mesures de gestion destinées à protéger l'accès aux connexions réseau et aux services en réseau;

d) les moyens utilisés pour accéder au réseau et aux services en réseau (par exemple les conditions à satisfaire pour un accès par réseau commuté à un fournisseur de services Internet ou à un système distant).

Il convient que la politique d'utilisation des services en réseau soit cohérente avec la politique de contrôle d'accès (voir 11.1).

Informations supplémentaires

Les connexions non autorisées et non sécurisées aux services en réseau peuvent nuire à l'ensemble de l'organisme. La mise en place de cette mesure est particulièrement importante pour les connexions réseau aux applications sensibles ou critiques, ou pour les utilisateurs se trouvant dans des lieux à haut risque, par exemple dans les lieux publics ou à l'extérieur des locaux soumis au contrôle du système de sécurité de l'organisme.

11.4.2 Authentification de l'utilisateur pour les connexions externes

Mesure

Il convient d'utiliser des méthodes d'authentification appropriées pour contrôler l'accès d'utilisateurs distants.

Préconisations de mise en œuvre

L'authentification des utilisateurs distants peut être réalisée, par exemple, à l'aide d'une technique cryptographique, de jetons ou d'un protocole «challenge/response». Ce type de techniques peut être mis en œuvre dans plusieurs solutions de réseaux privés virtuels (solutions VPN, de «virtual private networks»). Il est également possible d'utiliser des lignes privées dédiées garantissant la fiabilité des sources de connexion. Des procédures et des mesures de rappel automatique, par exemple via des modems de rappel automatique, peuvent également protéger les moyens de traitement de l'information d'un organisme contre les connexions non autorisées et indésirables. Ce type de mesure authentifie les utilisateurs qui tentent de se connecter au réseau d'un organisme à distance. Dans le cadre de cette mesure, il convient de ne pas utiliser des services en réseau incluant le renvoi automatique d'appels, ou si ces services sont utilisés, il convient de désactiver cette fonction afin d'éviter les failles qui lui sont associées. Il convient que le processus de rappel automatique soit accompagné d'une déconnexion du côté de l'organisme. Dans le cas contraire, l'utilisateur distant risque de laisser la ligne ouverte pour éviter une nouvelle authentification. Il convient que les procédures et mesures de rappel automatique soient entièrement soumises à essai sur ce point.

Le principe des nœuds d'authentification peut être utilisé pour des groupes d'utilisateurs distants connectés à un équipement partagé sécurisé. Les techniques cryptographiques, par exemple celles fondées sur les certificats machine, peuvent être utilisées pour l'authentification des nœuds. Ces techniques s'inscrivent dans le cadre des solutions VPN.

Il convient de mettre en œuvre des mesures d'authentification supplémentaires pour l'accès aux réseaux sans fil. Il est nécessaire d'accorder une attention particulière à la sélection des mesures destinées aux réseaux sans fil en raison des plus fortes probabilités d'interception et d'intrusion non détectées dans le réseau.

Informations supplémentaires

Les connexions externes constituent des possibilités d'accès non autorisé aux informations liées à l'activité de l'organisme, par exemple les accès par ligne commutée. Les différentes méthodes d'authentification offrent un niveau de protection plus ou moins élevé. Les méthodes fondées sur les techniques cryptographiques constituent un moyen d'authentification très efficace. Il est important de procéder à une appréciation du risque pour déterminer le niveau de protection requis, avant de choisir la méthode d'authentification appropriée.

Un équipement de connexion automatique à un ordinateur distant peut constituer une voie d'accès non autorisée à une application de gestion. Ce point est particulièrement important si la connexion utilise un réseau qui se trouve hors du contrôle du système de sécurité de l'organisme.

11.4.3 Identification des matériels en réseau

Mesure

Il convient de considérer l'identification automatique de matériels comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques.

Préconisations de mise en œuvre

L'identification de matériels peut être utilisée s'il est important de lancer la communication depuis un lieu ou un équipement spécifique. Un identifiant intégré dans le matériel ou associé à celui-ci peut être utilisé pour indiquer si la connexion du matériel au réseau est autorisée. Lorsque l'organisme comporte plusieurs réseaux et en particulier lorsque ces réseaux présentent des niveaux de sensibilité différents, il convient que ces identifiants indiquent clairement à quel réseau le matériel peut être connecté. Il peut être nécessaire d'envisager une protection physique du matériel pour assurer la sécurité de son identifiant.

Informations supplémentaires

Cette mesure peut être accompagnée d'autres techniques d'authentification de l'utilisateur du matériel (voir 11.4.2). L'identification du matériel peut être appliquée en complément de l'authentification de l'utilisateur.

11.4.4 Protection des ports de diagnostic et de configuration à distance

Mesure

Il convient de contrôler l'accès physique et logique aux ports de diagnostic et de configuration à distance.

Préconisations de mise en œuvre

Les contrôles potentiels de l'accès aux ports de diagnostic et de configuration à distance incluent l'utilisation d'une clé et de procédures d'accompagnement pour contrôler l'accès physique au port. Une procédure d'accompagnement possible consiste à faire en sorte que les ports de diagnostic et de configuration soient seulement accessibles après accord entre le responsable du service informatique et le personnel chargé de l'assistance matériel/logiciel demandant l'accès.

Il convient de désactiver ou de retirer les ports, services et équipements similaires installés sur un ordinateur ou un équipement en réseau qui ne sont pas spécifiquement requis pour la fonctionnalité de gestion.

Informations supplémentaires

De nombreux systèmes informatiques, systèmes réseau et systèmes de communication sont dotés d'un dispositif de diagnostic ou de configuration à distance à l'attention des techniciens de maintenance. Si ces ports ne sont pas protégés, ils constituent une voie potentielle d'accès non autorisée.

11.4.5 Cloisonnement des réseaux

Mesure

Il convient que les groupes de services d'information, d'utilisateurs et de systèmes d'information soient séparés sur le réseau.

Préconisations de mise en œuvre

Une méthode permettant de maîtriser la sécurité de réseaux de grande taille consiste à les subdiviser en domaines réseau logiques, par exemple un domaine réseau interne et un domaine réseau externe, chacun étant protégé par un périmètre de sécurité défini. Il est possible d'appliquer une série de mesures à différents domaines réseau logiques afin de compartimenter davantage les environnements de sécurité, par exemple en définissant des systèmes accessibles par le public, des réseaux internes et des réseaux critiques. Il convient de définir les domaines sur la base d'une appréciation du risque ainsi que les différentes exigences en matière de sécurité dans chaque domaine.

Pour mettre en œuvre un tel périmètre de sécurité, il est possible d'installer une passerelle sécurisée entre les deux réseaux à relier afin de contrôler l'accès et les flux d'information entre les deux domaines. Il convient de configurer cette passerelle afin de filtrer le trafic entre les deux domaines (voir 11.4.6 et 11.4.7) et de bloquer les accès non autorisés conformément à politique de contrôle d'accès de l'organisme (voir 11.1). Parmi les passerelles de ce type, citons le pare-feu. Une autre méthode de cloisonnement des domaines logiques consiste à limiter l'accès au réseau en définissant des réseaux virtuels privés destinés à des groupes d'utilisateurs, au sein de l'organisme.

Il est également possible de cloisonner des réseaux, par exemple à l'aide d'une commutation IP. Il est alors possible de mettre en œuvre les différents domaines en contrôlant les flux de données par le biais de fonctions de routage/commutation, telles que les listes de contrôle d'accès.

Il convient que les critères de cloisonnement des réseaux en domaines soient fondés sur la politique de contrôle d'accès et sur les exigences relatives à l'accès (voir 10.1), et qu'ils tiennent également compte du coût relatif et de l'impact sur les performances, liés à l'intégration d'un dispositif de routage ou d'une technologie de passerelle (voir 11.4.6 et 11.4.7).

En outre, il convient que le cloisonnement des réseaux repose sur la valeur et la classification des informations stockées ou traitées sur le réseau, les niveaux de confiance ou les politiques de gestion, afin de réduire l'impact de la défaillance d'un service sur l'ensemble de l'activité.

Il convient d'envisager de séparer les réseaux sans fil des réseaux internes et privés. Le périmètre des réseaux sans fil n'étant pas clairement défini, il convient de réaliser une appréciation du risque pour identifier les mesures qui permettront d'établir un cloisonnement (par exemple en mettant en place un niveau élevé d'authentification, des techniques cryptographiques et une sélection de la fréquence).

Informations supplémentaires

Les réseaux sont amenés à s'étendre de plus en plus au-delà des limites classiques des organismes, au gré des partenariats commerciaux, qui nécessitent l'interconnexion ou le partage de moyens de traitement de l'information et les moyens de réseautique. Ce type d'extension est susceptible d'augmenter le risque d'accès non autorisé aux systèmes d'information connectés au réseau, d'où la nécessité de mettre en place une protection pour certains systèmes particulièrement sensibles ou critiques.

11.4.6 Mesure relative à la connexion réseau

Mesure

Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, il convient de restreindre la capacité de connexion réseau des utilisateurs, conformément à la politique de contrôle d'accès et les exigences relatives aux applications de gestion (voir 11.1).

Préconisations de mise en œuvre

Il convient de tenir à jour les droits d'accès des utilisateurs, conformément à la politique de contrôle d'accès (voir 11.1.1).

La capacité de connexion des utilisateurs peut être restreinte à l'aide de passerelles réseau qui filtrent le trafic par le biais de tables ou de règles prédéfinies. Voici des exemples d'applications auxquelles il convient d'appliquer des restrictions:

a) les messageries électroniques;

b) les transferts de fichiers;

c) les accès interactifs;

d) les accès applicatifs.

Il convient d'envisager de lier les droits d'accès au réseau à certaines heures de la journée ou à certaines dates.

Informations supplémentaires

Pour les réseaux partagés, en particulier pour les réseaux qui s'étendent au-delà des limites de l'organisme, la politique de contrôle d'accès peut prévoir l'incorporation de mesures visant à restreindre la capacité de connexion des utilisateurs.

11.4.7 Contrôle du routage réseau

Mesure

Il convient de mettre en œuvre des mesures du routage des réseaux afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications de gestion.

Préconisations de mise en œuvre

Il convient que les mesures du routage soient fondées sur des mécanismes de vérification positive des adresses source et de destination.

Il est possible d'utiliser des passerelles de sécurité pour valider les adresses source et de destination aux points de contrôle internes et externes si des technologies de traduction d'adresses de serveurs mandataires et/ou réseau sont utilisées. Il convient que les personnes chargées de la mise en œuvre soient informées des avantages et des inconvénients des mécanismes déployés. Il convient que les exigences relatives au contrôle du routage réseau soient fondées sur la politique de contrôle d'accès (voir 11.1).

Informations supplémentaires

Les réseaux partagés, en particulier pour les réseaux qui s'étendent au-delà des limites de l'organisme, peuvent nécessiter des contrôles du routage supplémentaires. C'est notamment le cas pour les réseaux partagés avec des utilisateurs tiers (extérieurs à l'organisme).

11.5 Contrôle d'accès au système d'exploitation

Objectif: empêcher les accès non autorisés aux systèmes d'exploitation.

Il convient de mettre en place des dispositifs de sécurité pour restreindre l'accès aux systèmes d'exploitation aux seuls utilisateurs habilités. Il convient que ces dispositifs soient en mesure d'assurer les fonctions suivantes:

a) authentification des utilisateurs habilités, conformément à une politique de contrôle d'accès définie;

b) enregistrement des tentatives d'authentification réussies et avortées;

c) enregistrement des utilisations des privilèges spéciaux d'accès au système;

d) déclenchement d'alarmes en cas de violation des politiques de sécurité;

e) authentification par le biais de dispositifs appropriés;

f) le cas échéant, limitation du temps de connexion alloué aux utilisateurs.

11.5.1 Ouverture de sessions sécurisées

Mesure

Il convient que l'accès aux systèmes d'exploitation soit soumis à une procédure sécurisée d'ouverture de session.

Préconisations de mise en œuvre

Il convient que la procédure de connexion à un système d'exploitation soit conçue de manière à réduire le plus possible les possibilités d'accès non autorisé. Par conséquent, il convient que cette procédure de connexion ne dévoile que les informations minimales sur le système, afin de ne pas faciliter la tâche d'un éventuel utilisateur non habilité. Il convient qu'une procédure de connexion remplisse les fonctions suivantes:

a) ne faire mention à aucun moment du système ou de l'application tant que le processus de connexion n'est pas terminé;

b) afficher un avertissement général précisant que l'accès de l'ordinateur est limité aux seuls utilisateurs habilités;

c) ne pas proposer de messages d'aide pendant la procédure de connexion, qui pourraient faciliter un accès non autorisé;

d) valider les informations de connexion uniquement lorsque toutes les données auront été saisies. Si une condition d'erreur survient, il convient que le système n'indique pas quelle partie des données est correcte ou incorrecte;

e) limiter le nombre autorisé de tentatives de connexion avortées, par exemple trois tentatives, et pouvoir

   1) enregistrer les tentatives réussies et avortées,

   2) imposer un retard avant d'autoriser de nouvelles tentatives de connexion ou de rejeter toute tentative sans autorisation spécifique,

   3) débrancher les connexions de liaisons de données,

   4) envoyer un message d'alarme à la console système si le nombre maximal de tentatives de connexion est atteint,

   5) définir le nombre de tentatives de saisie du mot de passe en fonction de la longueur minimale du mot de passe et de la valeur du système à protéger;

f) définir le temps maximal et le temps minimal autorisés pour la procédure de connexion. Si ce temps est dépassé, il convient que le système mette un terme à la connexion;

g) afficher les informations suivantes après une connexion réussie:

   1) la date et l'heure de la dernière connexion réussie;

   2) les détails relatifs à toute tentative de connexion avortée depuis la dernière tentative réussie;

h) ne pas afficher le mot de passe en cours de saisie, ou bien pouvoir masquer le mot de passe en affichant des symboles;

i) ne pas transmettre les mots de passe au sein d'un réseau sous la forme d'un texte en clair.

Informations supplémentaires

Si les mots de passe sont transmis sous forme d'un texte en clair pendant la session de connexion à un réseau, ils risquent d'être capturé par un analyseur de réseau.

11.5.2 Identification et authentification de l'utilisateur

Mesure

Il convient d'attribuer à chaque utilisateur un identifiant unique et exclusif et de choisir une technique d'authentification permettant de vérifier l'identité déclarée par l'utilisateur.

Préconisations de mise en œuvre

Il convient d'appliquer cette mesure à tous les types d'utilisateurs (y compris au personnel de l'assistance technique, aux opérateurs, aux administrateurs réseau, aux programmeurs système et aux administrateurs de base de données).

Il convient d'utiliser les identifiants utilisateurs pour suivre leurs opérations et retrouver les éventuelles responsabilités. Il convient que les activités ordinaires des utilisateurs ne soient pas réalisées à l'aide d'un compte doté de privilèges.

Dans des cas exceptionnels répondant à des impératifs de gestion, il est possible d'utiliser un identifiant partagé créé pour un groupe d'utilisateurs ou une tâche spécifique. Dans de tels cas de figure, il convient de documenter l'accord de la direction. Des mesures supplémentaires peuvent être requises pour garantir l'imputabilité.

Il convient d'autoriser des identifiants génériques pour un utilisateur donné uniquement lorsqu'il n'est pas nécessaire que les fonctions accessibles ou les opérations réalisées par l'identifiant soient traçables (par exemple en accès en lecture seule), ou bien lorsqu'il existe d'autres mesures (par exemple un mot de passe pour un identifiant générique est attribué exclusivement à un seul collaborateur à la fois et cette instance est journalisée).

Lorsqu'un niveau élevé d'authentification et d'identification est requis, il convient d'utiliser des méthodes d'authentification autres que les mots de passe (par exemple un dispositif cryptographique tel qu'une carte à puce, des jetons d'authentification ou des techniques de biométrie).

Informations supplémentaires

Les mots de passe (voir également 11.3.1 et 11.5.3) sont un moyen d'identification et d'authentification très courant, fondé sur un secret connu de l'utilisateur seul. Il est possible d'obtenir le même résultat avec des moyens cryptographiques et des protocoles d'authentification. Il convient d'adapter le niveau d'identification et d'authentification de l'utilisateur en fonction de la sensibilité des informations auxquelles on souhaite accéder.

Les identifiants matériels de type jetons ou cartes à puce peuvent également servir de moyen d'identification et d'authentification. La biométrie, qui utilise les caractéristiques ou attributs uniques d'un individu, peut également être utilisée pour identifier une personne. Une combinaison sécurisée de ces technologies et mécanismes offre un niveau d'authentification plus élevé.

11.5.3 Système de gestion des mots de passe

Mesure

Il convient que les systèmes qui gèrent les mots de passe soient interactifs et fournissent des mots de passe de qualité.

Préconisations de mise en œuvre

Il convient qu'un système de gestion des mots de passe ait les propriétés suivantes:

a) mettre en vigueur l'utilisation d'identifiants et de mots de passe utilisateurs individuels afin de garantir l'imputabilité;

b) autoriser l'utilisateur à choisir et à modifier ses mots de passe, et inclure une procédure de confirmation afin de tenir compte des éventuelles erreurs de saisie;

c) imposer le choix de mots de passe de qualité (voir 11.3.1);

d) mettre en vigueur le principe du changement de mot de passe (voir 11.3.1);

e) imposer aux utilisateurs de changer un mot de passe temporaire dès la première connexion (voir 11.2.3);

f) tenir à jour un enregistrement des anciens mots de passe utilisateurs et empêcher leur réutilisation;

g) ne pas afficher les mots de passe à l'écran lors de leur saisie;

h) stocker les fichiers de mots de passe à d'autres emplacements que les données de l'application;

i) stocker et transmette les mots de passe sous une forme protégée (par exemple par chiffrement ou hachage).

Informations supplémentaires

Les mots de passe sont l'un des principaux moyens permettant de valider les droits d'utilisation d'un utilisateur pour l'accès à un service de son ordinateur.

Certaines applications nécessitent que l'attribution de mots de passe aux utilisateurs soit réalisée par une autorité indépendante; dans ce cas, les points b), d) et e) ci-avant ne s'appliquent pas. La plupart du temps, les mots de passe sont choisis et gérés par les utilisateurs eux-mêmes. Pour un complément d'information sur l'utilisation des mots de passe, voir 11.3.1.

11.5.4 Emploi des utilitaires système

Mesure

Il convient de limiter et de contrôler étroitement l'emploi des programmes utilitaires permettant de contourner les mesures d'un système ou d'une application.

Préconisations de mise en œuvre

Il convient de tenir compte des directives suivantes concernant l'emploi des utilitaires:

a) utiliser les procédures d'identification, d'authentification et d'autorisation spécifiques aux utilitaires système;

b) séparer les utilitaires des logiciels d'application;

c) limiter l'emploi des utilitaires au nombre minimal d'utilisateurs de confiance bénéficiant d'une autorisation (voir également 11.2.2);

d) autoriser une utilisation *ad hoc* des utilitaires;

e) limiter la disponibilité des utilitaires, par exemple limiter la durée d'une autorisation de modification;

f) journaliser toutes les utilisations d'utilitaires système;

g) définir et documenter les niveaux d'autorisation relatifs aux utilitaires;

h) désinstaller ou désactiver tous les utilitaires logiciels et logiciels système inutiles;

i) ne pas mettre d'utilitaires système à la disposition des utilisateurs disposant d'un accès à des applications stockées sur des systèmes pour lesquels la séparation des tâches est requise.

Informations supplémentaires

La plupart des installations informatiques comportent un ou plusieurs programme(s) utilitaire(s) susceptible(s) de contourner les mesures d'un système ou d'une application.

11.5.5 Déconnexion automatique des sessions inactives

Mesure

Il convient que les sessions inactives soient déconnectées après une période d'inactivité définie.

Préconisations de mise en œuvre

Au terme d'une période d'inactivité définie, il convient qu'un dispositif de déconnexion réinitialise la fenêtre d'ouverture de session, puis ferme éventuellement les sessions applicatives et les sessions réseau. Il convient que le délai de déconnexion reflète le niveau de risque lié à la sécurité, la classification des informations manipulées et des applications utilisées, ainsi que les risques liés aux utilisateurs des matériels.

Un dispositif de déconnexion simplifié peut être prévu pour certains systèmes, qui réinitialise la fenêtre d'ouverture de session et empêche l'accès non autorisé, mais ne ferme pas les sessions applicatives ni les applications réseau.

Informations supplémentaires

Cette mesure est particulièrement importante dans les lieux à haut risque, par exemple dans les lieux publics ou les zones extérieures qui échappent au contrôle du système de sécurité de l'organisme. Il convient que les sessions soient déconnectées afin d'empêcher l'accès de personnes non habilitées et de contrer les attaques par refus de service.

11.5.6 Limitation du temps de connexion

Mesure

Il convient de restreindre les temps de connexion afin d'apporter un niveau de sécurité supplémentaire aux applications à haut risque.

Préconisations de mise en œuvre

Il convient d'envisager des restrictions du temps de connexion pour les applications sensibles, notamment pour celles se trouvant dans les lieux à haut risque, par exemple dans les lieux publics ou les zones extérieures qui échappent au contrôle du système de sécurité de l'organisme. Voici des exemples de restriction du temps de connexion:

a) utilisation d'intervalles de temps prédéterminés, par exemple pour les besoins d'une transmission par lots ou pour des sessions interactives ordinaires de courte durée;

b) restriction des temps de connexion aux horaires de bureau normaux, lorsque l'activité de l'organisme ne nécessite par d'heures supplémentaires ou d'heures d'ouverture prolongées;

c) mise en place d'une procédure de réauthentification à intervalles prédéfinis.

Informations supplémentaires

La limitation de la période pendant laquelle les connexions aux services de l'ordinateur sont autorisées permet de réduire les probabilités d'accès non autorisé. Le fait de limiter la durée des sessions actives empêche les utilisateurs de garder leur session ouverte pour éviter d'avoir à se réauthentifier.

11.6 Contrôle d'accès aux applications et à l'information

Objectif: empêcher les accès non autorisés aux informations stockées dans les applications.

Il convient de mettre en place des dispositifs de sécurité pour restreindre l'accès aux applications et la navigation au sein des applications.

Il convient de restreindre l'accès logique aux logiciels d'application et aux informations aux seuls utilisateurs habilités. Il convient que les applications comprennent les fonctions suivantes:

a) contrôler l'accès utilisateur aux informations et aux fonctions applicatives, conformément à une politique de contrôle d'accès;

b) assurer une protection contre les accès non autorisés via tout utilitaire, logiciel d'exploitation ou logiciel malveillant à même de contourner ou de court-circuiter les mesures système ou d'application;

c) ne pas constituer un risque pour les autres systèmes avec lesquels les applications partagent des informations.

11.6.1 Restriction d'accès à l'information

Mesure

Pour les utilisateurs et le personnel chargé de l'assistance technique, il convient de restreindre l'accès aux informations et aux fonctions applicatives conformément à la politique de contrôle d'accès.

Préconisations de mise en œuvre

Il convient de fonder les restrictions d'accès sur des exigences de gestion définies au cas par cas. Il convient que la politique de contrôle d'accès soit également compatible avec la politique de contrôle d'accès physique aux locaux de l'organisme (voir 11.1).

Il convient d'envisager l'application des lignes directrices suivantes afin d'appuyer les exigences relatives aux restrictions d'accès:

a) créer des menus permettant de contrôler l'accès aux fonctions de l'application;

b) contrôler les droits d'accès des utilisateurs, par exemple: lecture, écriture, suppression et exécution;

c) contrôler les droits d'accès aux autres applications;

d) pour les applications traitant des informations sensibles, veiller à ce que les données de sortie contiennent uniquement les informations nécessaires à l'utilisation des données de sortie et soient envoyées uniquement aux terminaux et autres destinataires habilités; il convient que ce processus prévoie des réexamens périodiques de ces données de sortie afin de supprimer les informations redondantes.

11.6.2 Isolement des systèmes sensibles

Mesure

Il convient que les systèmes sensibles disposent d'un environnement informatique dédié (isolé).

Préconisations de mise en œuvre

Pour les besoins de l'isolement des systèmes sensibles, il convient de prendre en compte les points suivants:

a) il convient que le propriétaire de l'application identifie et documente clairement la sensibilité de l'application (voir 7.1.2);

b) lorsqu'une application sensible doit être exploitée dans un environnement partagé, il convient que le propriétaire de l'application sensible identifie et accepte les applications avec lesquelles elle partage ses ressources, ainsi que le risque associé.

Informations supplémentaires

Le niveau de sensibilité de certaines applications nécessite une manipulation spéciale. Il peut être nécessaire

a) d'utiliser un ordinateur dédié, ou

b) de partager des ressources uniquement avec des applications dont la fiabilité est reconnue.

L'isolement peut être réalisé à l'aide de méthodes physiques ou logiques (voir également 11.4.5).

11.7 Informatique mobile et télétravail

Objectif: garantir la sécurité de l'information lors de l'utilisation d'appareils informatiques mobiles et d'équipements de télétravail.

Il convient d'assurer un niveau de protection adapté aux risques liés à ce mode de fonctionnement. L'utilisation d'appareils informatiques mobiles nécessite la prise en compte d'un environnement de travail non protégé et la mise en place d'une protection appropriée. Dans le cas du télétravail, il convient de protéger le site de travail et de veiller à la mise en place d'installations appropriées.

11.7.1 Informatique mobile et télécommunications

Mesure

Il convient de mettre en place une procédure formelle et des mesures de sécurité appropriées pour assurer une protection contre le risque lié à l'utilisation d'appareils informatiques et de communication mobiles.

Préconisations de mise en œuvre

Lorsque des appareils informatiques et de communication mobiles sont utilisés, par exemple un ordinateur bloc-notes, un ordinateur de poche, un ordinateur portable, une carte à puce ou un téléphone mobile, la protection des informations liées à l'activité de l'organisme nécessite une attention particulière. Il convient que la politique relative aux appareils informatiques mobiles tienne compte des risques liés à l'utilisation de ce type d'appareils dans des environnements non protégés, c'est-à-dire qu'elle prévoie une protection physique, des contrôles d'accès, des techniques cryptographiques, des sauvegardes et une protection antivirus. Il convient que cette politique prévoie également des règles et des recommandations relatives à la connexion des appareils au réseau, ainsi que des conseils sur l'utilisation de ces appareils dans les lieux publics, dans les salles de réunion et en tout autre lieu non protégé situé hors des locaux de l'organisme. Les mesures de protection visent à empêcher les accès non autorisés aux informations stockées et traitées par ces appareils ainsi que la divulgation de ces informations. La mise en place de techniques cryptographiques (voir 12.3) est un exemple de protection.

Il convient que les personnes utilisant un appareil informatique mobile dans un lieu public veillent à protéger l'écran des regards indiscrets. Il convient de mettre en place et de tenir à jour des procédures de protection contre les logiciels malveillants (voir 10.4).

Il convient de réaliser, à intervalles réguliers, des sauvegardes des informations critiques liées à l'activité de l'organisme. À cet effet, il convient d'installer des équipements permettant une procédure de sauvegarde rapide et simple. Il convient de protéger ces sauvegardes contre des risques tels que le vol ou la perte d'informations.

Il convient de prévoir une protection appropriée dans le cas des appareils informatiques mobiles disposant d'une connexion réseau. Pour les informations liées à l'activité de l'organisme stockées sur un réseau public, il convient d'accorder l'accès distant via un appareil informatique mobile uniquement après une identification et une authentification réussies et s'il existe un mécanisme de contrôle d'accès approprié (voir 11.4).

Il convient que les appareils informatiques mobiles soient physiquement protégés contre le vol, en particulier lorsqu'ils sont laissés dans un véhicule privé ou tout autre moyen de transport, une chambre d'hôtel, un centre de congrès ou une salle de réunion. Il convient d'établir une procédure tenant compte de la police d'assurance et des exigences légales et de sécurité spécifiques à l'organisme, en cas de vol ou de perte d'un appareil informatique mobile. Il convient de ne pas laisser sans surveillance les équipements dans lesquels sont stockées des informations importantes, sensibles et/ou critiques liées à l'activité de l'organisme et, dans la mesure du possible, de les mettre sous clé ou de les doter de serrures spéciales (voir 9.2.5).

Il convient d'organiser des formations pour sensibiliser les personnes utilisant des appareils informatiques mobiles aux risques supplémentaires liés à ce mode de travail et sur les mesures de sécurité qu'il convient de mettre en œuvre.

Informations supplémentaires

Les connexions sans fil des appareils mobiles reposent sur le même principe que les autres types de connexion réseau. Cependant, elles présentent des spécificités importantes qu'il convient de prendre en compte lors de la définition des mesures de sécurité:

a) certains protocoles de sécurité sans fil sont en phase de rodage et leurs failles sont connues;

b) la sauvegarde des informations stockées sur les appareils informatiques mobiles n'est pas toujours possible en raison d'une bande passante limitée et/ou parce que les appareils mobiles ne sont pas connectés au moment où les sauvegardes automatiques sont lancées.

11.7.2 Télétravail

Mesure

Il convient d'élaborer et de mettre en œuvre une politique, des procédures et des programmes opérationnels spécifiques au télétravail.

Préconisations de mise en œuvre

Il convient que l'organisme autorise le télétravail uniquement s'il considère qu'il existe des dispositions de sécurité appropriées, conformes à la politique de sécurité.

Il convient de protéger le site de télétravail contre des risques tels que le vol de matériel et d'informations, la diffusion non autorisée d'informations, l'accès distant non autorisé aux systèmes ou le mauvais usage des équipements. Il convient que les activités du télétravailleur soient à la fois autorisées et contrôlées par la direction et il convient de mettre en place les mesures adaptées à ce type d'activité.

Il convient de tenir compte des points suivants:

a) le niveau de sécurité physique existant sur le site de télétravail, y compris le niveau de sécurité physique du bâtiment et de l'environnement immédiat;

b) l'environnement physique de télétravail;

c) les exigences en matière de sécurité des télécommunications, en tenant compte de la nécessité d'accéder à distance aux systèmes internes de l'organisme, de la sensibilité des informations consultées ou transmises via les liaisons téléinformatiques et de la sensibilité du système interne;

d) la menace d'accès non autorisé aux informations ou ressources par d'autres personnes présentes;

e) l'utilisation de réseaux domestiques et les exigences ou les restrictions relatives à la configuration des réseaux sans fil;

f) les politiques et procédures mises au point pour empêcher tout litige sur les droits sur les propriétés intellectuelles concernant des biens créés sur un matériel privé;

g) l'accès au matériel personnel (pour vérifier le niveau de sécurité de la machine ou lors d'une enquête), susceptible d'être interdit par la loi;

h) les contrats de licence logicielles faisant apparaître que l'organisme peut être responsable de l'octroi des licences pour les logiciels clients des postes de travail privés des salariés, des contractants et des utilisateurs tiers;

i) les exigences relatives à la protection antivirus et au pare-feu.

Il convient d'examiner les lignes directrices et les dispositions suivantes:

a) lorsque l'utilisation d'un matériel personnel non soumis au contrôle de l'organisme est interdite, fournir un matériel et un meuble de rangement adaptés au télétravail;

b) définir les tâches autorisées, les heures de travail, la classification des informations susceptibles d'être détenues, ainsi que les systèmes et services internes auxquels le télétravailleur a accès;

c) fournir un appareil de communication approprié, ainsi que des méthodes de sécurisation de l'accès distant;

d) la sécurité physique;

e) les règles et recommandations concernant l'accès de la famille et des visiteurs au matériel et aux informations;

f) la fourniture de services d'assistance et de maintenance matérielle et logicielle;

g) la souscription à une assurance;

h) les procédures de sauvegarde et de gestion de la continuité de l'activité;

i) l'audit et la surveillance liée à la sécurité;

j) la révocation des droits d'utilisation et des droits d'accès, ainsi que la restitution du matériel au terme des activités de télétravail.

Informations supplémentaires

Le télétravail utilise la technologie des télécommunications pour permettre au personnel de travailler depuis un site fixe distant, en dehors des locaux de l'organisme.

12 Acquisition, développement et maintenance des systèmes d'information

12.1 Exigences de sécurité applicables aux systèmes d'information

Objectif: veiller à ce que la sécurité fasse partie intégrante des systèmes d'information.

Les systèmes d'information comprennent des systèmes d'exploitation, une infrastructure, des applications de gestion, des produits «clé en main», des services et des applications mises au point par les utilisateurs. La conception et la mise en œuvre du système d'information prenant en charge le processus métier peuvent être critiques pour la sécurité. Il convient que les exigences de sécurité soient identifiées et définies avant la phase de développement et/ou de mise en œuvre des systèmes d'information.

Il convient que toutes les exigences de sécurité soient identifiées en même temps que les exigences générales d'un projet et qu'elles soient justifiées, reconnues et documentées dans le cadre de la gestion générale d'un système d'information.

12.1.1 Analyse et spécification des exigences de sécurité

Mesure

Il convient que les exigences métier relatives aux nouveaux systèmes d'information ou que les améliorations apportées aux systèmes d'information existants spécifient les exigences de sécurité.

Préconisations de mise en œuvre

Il convient que les spécifications relatives aux mesures de sécurité prévoient l'intégration de mesures automatisées dans le système d'information et tiennent compte de la nécessité de les accompagner par des mesures manuelles. Il convient d'appliquer des considérations similaires lors de l'évaluation des progiciels développés ou achetés pour les applications de gestion.

Il convient que les exigences de sécurité et les mesures reflètent la valeur des actifs informationnels concernés (voir également 7.2), ainsi que les éventuels préjudices pour l'activité de l'organisme en cas de défaillance ou d'absence de sécurité.

Dans le cadre d'un projet portant sur les systèmes d'information, il convient d'intégrer les exigences système en matière de sécurité et les processus de mise en œuvre de la sécurité lors des phases initiales du projet. Les mesures introduites lors de la phase de conception sont considérablement moins onéreuses à mettre en œuvre et à gérer que celles ajoutées pendant ou après la mise en œuvre.

Si les produits sont achetés, il convient de suivre un processus formel de mise à l'essai et d'acquisition. Dans les contrats conclus avec le fournisseur, il convient de prendre en compte les exigences de sécurité identifiées. Lorsque le produit proposé dispose d'une fonctionnalité de sécurité insuffisante au regard des exigences spécifiées, alors il convient de réexaminer le risque et les mesures associées avant d'acheter ce produit. Lorsqu'une fonctionnalité supplémentaire est fournie et engendre un risque au niveau de la sécurité, il convient de la désactiver ou de réexaminer la structure de contrôle proposée afin de déterminer s'il est possible de tirer profit de la fonctionnalité disponible.

Informations supplémentaires

Le cas échéant, par exemple pour des raisons de coût, la direction peut choisir d'utiliser des produits évalués et certifiés par un organisme indépendant. Pour de plus amples informations sur les critères d'évaluation des produits de sécurité des systèmes d'information, voir l'ISO/CEI 15408 ou d'autres normes d'évaluation ou de certification, le cas échéant.

L'ISO/CEI TR 13335-3 fournit des recommandations sur l'utilisation de méthodes de management du risque en vue d'identifier les exigences relatives aux mesures de sécurité.

12.2 Bon fonctionnement des applications

Objectif: empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans les applications.

Pour garantir un bon traitement des informations, il convient d'intégrer des mesures appropriées dans les applications, y compris dans les applications mises au point par les utilisateurs. Il convient que ces mesures prévoient la validation des données d'entrée, du traitement interne et des données de sortie.

Des mesures supplémentaires peuvent être requises pour les systèmes qui traitent ou qui ont une incidence sur les informations sensibles, critiques ou ayant une valeur pour l'organisme. Il convient que ces mesures soient déterminées sur la base des exigences de sécurité et l'appréciation du risque.

12.2.1 Validation des données d'entrée

Mesure

Il convient de valider les données entrées dans les applications afin de vérifier si elles sont correctes et appropriées.

Préconisations de mise en œuvre

Il convient de vérifier les données portant sur les transactions commerciales, les informations de référence (telles que nom, adresse, plafond de crédit, numéros de référence clients) et les tables de paramètres (comme les prix de vente, les taux de change, les taux d'imposition). Il convient de tenir compte des directives suivantes:

a) la vérification des données saisies en double ou autres vérifications, par exemple en vérifiant les valeurs-limites ou en limitant les champs à des intervalles de saisies, afin de détecter les erreurs suivantes:

   1) les valeurs hors intervalle;

   2) les caractères invalides dans les champs de données;

   3) les données manquantes ou incomplètes;

   4) non respect des limites inférieures et supérieures en terme de volume;

   5) paramètre de mesures de sécurité non autorisés ou incohérents;

b) le réexamen périodique du contenu des champs-clés ou des fichiers de données pour confirmer leur validité et leur intégrité;

c) la recherche des éventuelles modifications non autorisées dans les exemplaires papier des documents d'entrée (il convient que tous les changements apportés aux documents d'entrée fassent l'objet d'une autorisation);

d) les procédures à appliquer en cas d'erreurs de validation;

e) les procédures visant à évaluer la vraisemblance des données d'entrée;

f) la définition des responsabilités de tout le personnel concerné par la saisie des données;

g) la création d'un journal des activités liées à la saisie de données (voir 10.10.1).

Informations supplémentaires

Le cas échéant, l'examen et la validation automatique des données d'entrée peuvent être envisagés, afin de réduire le risque d'erreurs et d'empêcher les attaques classiques, comme les attaques par dépassement de la mémoire tampon et l'injection de code malveillant.

12.2.2 Mesure relative au traitement interne

Mesure

Il convient d'inclure des mesures de validation dans les applications afin de détecter les éventuelles altérations de l'information dues à des erreurs de traitement ou des actes délibérés.

Préconisations de mise en œuvre

Il convient que la conception et la mise en œuvre des applications visent à réduire le plus possible les risques de défaillance donnant lieu à des pertes d'intégrité. Les domaines concernés sont les suivants:

a) l'utilisation des fonctions «ajouter», «modifier» et «supprimer» pour appliquer des modifications aux données;

b) les procédures destinées à empêcher le mauvais ordre d'exécution des programmes leur exécution après échec d'un traitement antérieur (voir également 10.1.1);

c) à la suite d'un échec, l'utilisation de programmes appropriés, afin de garantir le bon traitement des données;

d) une protection contre les attaques par dépassement de la mémoire tampon.

Il convient d'établir une liste de contrôle, de documenter les activités et de conserver les résultats en lieu sûr. Les vérifications peuvent porter sur les éléments suivants:

a) les contrôles de session ou de lots, destinés à rapprocher les soldes de fichiers de données après une mise à jour des transactions;

b) les mesures d'équilibrage, pour comparer les soldes d'ouverture aux soldes de clôture, à savoir:

   1) les commandes «run-to-run» (échange de paramètres intermédiaires);

   2) les totaux de mises à jour de fichier;

   3) les commandes programme à programme;

c) la validation des données d'entrée générées par le système (voir 12.2.1);

d) la vérification de l'intégrité, de l'authenticité (ou de toute autre caractéristique liée à la sécurité) des données ou du logiciel téléchargé(es) d'un ordinateur central vers un ordinateur distant et inversement;

e) les totaux mêlés pour les enregistrements et les fichiers;

f) les vérifications permettant de garantir que les programmes s'exécutent au bon moment;

g) les opérations permettant de garantir le bon séquencement des programmes, l'interruption des programmes en cas d'échec et l'arrêt de tout traitement jusqu'à résolution du problème;

h) la création d'un journal des activités liées au traitement (voir 10.10.1).

Informations supplémentaires

Des données correctement saisies peuvent être altérées en raison d'un défaut du support physique ou à la suite d'une erreur de traitement ou d'un acte délibéré. Les procédures de validation requises dépendent de la nature de l'application et de l'impact d'une éventuelle altération des données sur l'activité de l'organisme.

12.2.3 Intégrité des messages

Mesure

Il convient d'identifier les exigences relatives à l'authentification et à la protection de l'intégrité des messages. Il convient également d'identifier et de mettre en œuvre les mesures appropriées.

Préconisations de mise en œuvre

Il convient de conduire une appréciation du risque lié à la sécurité pour déterminer si l'intégrité du message est requise et pour identifier la méthode de mise en œuvre la plus appropriée.

Informations supplémentaires

Il est possible d'utiliser des techniques cryptographiques (voir 12.3) pour assurer l'authentification des messages.

12.2.4 Validation des données de sortie

Mesure

Il convient de valider les données de sortie d'une application pour vérifier que le traitement des informations stockées est correct et adapté aux circonstances.

Préconisations de mise en œuvre

La validation des données de sortie peut inclure ce qui suit:

a) des contrôles de vraisemblance, pour vérifier si les données de sortie ont des valeurs admissibles;

b) des décomptes de contrôle des rapprochements pour garantir le traitement de toutes les données;

c) suffisamment d'informations pour permettre à un utilisateur ou un système de traitement de déterminer l'exactitude, l'exhaustivité, la précision et la classification de l'information;

d) après les essais de validation des données de sortie, d'éventuelles actions correctives;

e) la définition des responsabilités de tout le personnel concerné par le traitement des données de sortie;

f) la création d'un journal des activités dans le cadre du processus de validation des données de sortie.

Informations supplémentaires

Généralement, les systèmes et applications sont bâtis sur l'hypothèse selon laquelle des procédures de validation, de vérification et d'essai appropriées permettent d'obtenir des données de sorties toujours correctes. Toutefois, cette hypothèse n'est pas toujours valide; dans certains cas, les systèmes soumis à essai peuvent continuer à générer des données incorrectes.

12.3 Mesures cryptographiques

Objectif: protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques.

Il convient d'élaborer une politique d'utilisation des mesures cryptographiques. Il convient de créer une procédure de gestion des clés pour mettre en œuvre les techniques cryptographiques.

12.3.1 Politique d'utilisation des mesures cryptographiques

Mesure

Il convient d'élaborer et de mettre en œuvre une politique d'utilisation des mesures cryptographiques en vue de protéger l'information.

Préconisations de mise en œuvre

Lors de l'élaboration d'une méthode cryptographique, il convient de tenir compte des éléments suivants:

a) la politique de la direction concernant l'utilisation de mesures cryptographiques au sein de l'organisme, y compris les principes généraux de protection des informations liées à l'activité de l'organisme (voir également 5.1.1);

b) sur la base d'une appréciation du risque, il convient d'identifier le niveau de protection requis en tenant compte du type, de la puissance et de la qualité de l'algorithme de chiffrement requis;

c) l'utilisation d'une technique de chiffrement, en vue de protéger les informations sensibles stockées sur un support amovible ou mobile ou acheminées par des voies d'intercommunication;

d) la politique en matière de gestion des clés, notamment les méthodes à utiliser pour protéger les clés de chiffrement et récupérer des informations chiffrées en cas de perte, de compromission ou d'endommagement des clés;

e) les rôles et les responsabilités, concernant notamment:

   1) la mise en œuvre de la politique de chiffrement;

   2) la gestion des clés, notamment la génération des clés (voir également 12.3.2);

f) les normes à adopter pour une mise en œuvre efficace dans l'ensemble de l'organisme (quelle solution est utilisée pour quel processus métier);

g) l'incidence du chiffrement des informations dans le cas des mesures reposant sur l'analyse du contenu (par exemple la détection de virus).

Lors de la mise en œuvre de la politique de chiffrement des informations, il convient de tenir compte des restrictions réglementaires et nationales pouvant s'appliquer aux techniques cryptographiques dans différentes régions du monde, ainsi que des questions de flux transfrontières des informations chiffrées (voir également 15.1.6).

Il est possible d'utiliser des mesures cryptographiques pour différents impératifs de sécurité, tels que les suivants:

a) confidentialité: le chiffrement des données permet de protéger des informations sensibles ou critiques, durant leur stockage ou leur transmission;

b) intégrité/authenticité: l'utilisation de signatures électroniques ou de codes d'authentification de message permet de protéger l'authenticité et l'intégrité des informations sensibles ou critiques, durant leur stockage ou leur transmission;

c) non-répudiation: l'utilisation de techniques cryptographiques permet d'établir la preuve de la survenue ou la non-survenue d'un événement ou d'une action.

Informations supplémentaires

Il convient que la décision d'utiliser une solution cryptographique s'inscrive dans le cadre d'un processus plus large d'appréciation du risque et de sélection des mesures. Cette appréciation peut donc être utilisée pour déterminer l'adéquation d'une mesure cryptographique, le type de mesure qu'il convient d'appliquer, dans quel but et pour quel processus métier.

Une politique d'utilisation des mesures cryptographiques permet d'optimiser les avantages du chiffrement, de réduire le plus possible les risques associés, et d'éviter un mauvais usage. Lors de l'utilisation de signatures électroniques, il convient de tenir compte des dispositions légales applicables, notamment la législation définissant les conditions dans lesquelles la signature électronique a force d'obligation (voir 15.1).

Il convient de consulter un spécialiste afin d'identifier le niveau de protection adéquat et de définir les spécifications appropriées qui garantiront ce niveau de protection et permettront la mise en œuvre d'un système sécurisé de gestion des clés (voir également 12.3.2).

L'ISO/CEI JTC1 SC27 a élaboré plusieurs normes relatives aux mesures cryptographiques. Pour plus ample information, voir l'IEEE P1363 et les Lignes directrices de l'OCDE relatives à la cryptographie.

12.3.2 Gestion des clés

Mesure

Il convient qu'une procédure de gestion des clés vienne à l'appui de la politique de l'organisme en matière de chiffrement.

Préconisations de mise en œuvre

Il convient de protéger toutes les clés de chiffrement contre toute modification, perte ou destruction. En outre, il est nécessaire de protéger les clés secrètes et personnelles contre toute divulgation non autorisée. Il convient de prévoir une protection physique pour le matériel utilisé pour générer, stocker et archiver les clés.

Il convient que le système de gestion des clés repose sur une série de normes, de procédures et de méthodes sécurisées en vue des actions suivantes:

a) générer des clés pour divers systèmes cryptographiques et diverses applications;

b) générer et obtenir des certificats de clés publiques;

c) distribuer des clés aux utilisateurs habilités et leur indiquer le mode d'activation à la remise des clés;

d) stocker des clés, notamment définir le mode d'attribution des clés;

e) mettre à jour ou remplacer les clés, notamment les règles régissant le remplacement des clés et la procédure à suivre;

f) traiter les clés compromises;

g) révoquer les clés, notamment définir le mode de retrait ou de désactivation des clés, par exemple lorsque les clés sont compromises ou lorsqu'un utilisateur quitte l'organisme (dans ce cas, il convient d'archiver les clés);

h) récupérer les clés perdues ou altérées dans le cadre du plan de continuité de l'activité, par exemple pour la récupération des informations chiffrées;

i) archiver les clés, par exemple pour les informations archivées ou sauvegardées;

j) détruire les clés;

k) journaliser et auditer les activités liées à la gestion des clés.

Afin de réduire la probabilité de compromission, il convient de fixer des dates d'activation et de désactivation des clés; ainsi, les clés ne peuvent être utilisées que pour une période limitée. Il convient que cette période soit adaptée au risque identifié et aux circonstances dans lesquelles la mesure cryptographique est mise en œuvre.

Outre la gestion sécurisée des clés secrètes et personnelles, il convient de tenir compte de l'authenticité des clés publiques. Ce processus d'authentification peut être mis en œuvre à l'aide de certificats de clés publiques, généralement délivrés par une autorité de certification. Il convient que cette dernière soit un organisme reconnu disposant de mesures et de procédures appropriées qui garantissent le degré de fiabilité requis.

Il convient que les accords de service ou contrats conclus avec des fournisseurs externes de services cryptographiques, comme par exemple une autorité de certification, couvrent les questions de responsabilité juridique, de fiabilité des services et de réactivité dans la fourniture de ces services (voir 6.2.3).

Informations supplémentaires

La gestion des clés de chiffrement est essentielle à l'efficacité des techniques cryptographiques. Voir l'ISO/CEI 11770 pour plus ample information sur la gestion des clés. Il existe deux types de techniques cryptographiques:

a) la cryptographie à clé secrète: plusieurs parties partagent la même clé pour chiffrer et déchiffrer les informations; cette clé doit rester secrète car toute personne ayant accès à la clé est en mesure de déchiffrer toutes les informations chiffrées avec cette clé ou d'introduire des informations non autorisées;

b) la cryptographie à clé publique: chaque utilisateur possède une paire de clés, une clé publique (qui peut être connue de tous) et une clé privée (qui doit rester secrète). Les techniques à clé publique peuvent être utilisées pour le chiffrement et pour générer des signatures électroniques (voir également l'ISO/CEI 9796 et l'ISO/CEI 14888-1).

Il est possible de falsifier une signature électronique en la remplaçant par une clé publique. L'utilisation d'un certificat de clé publique permet de remédier à ce problème.

Les techniques cryptographiques peuvent également être utilisées pour protéger les clés cryptographiques. Il peut s'avérer nécessaire d'élaborer des procédures pour répondre à des exigences légales d'accès aux clés cryptographiques, par exemple pour décrypter des informations qui serviront de preuve dans le cadre d'un procès.

12.4 Sécurité des fichiers système

Objectif: garantir la sécurité des fichiers système.

Il convient de contrôler l'accès aux fichiers système et au code source du programme et de conduire les projets informatiques et les activités d'assistance conformément aux exigences de sécurité. Il convient de veiller à ne pas exposer les données sensibles dans des environnements d'essai.

12.4.1 Mesure relative aux logiciels en exploitation

Mesure

Il convient de mettre des procédures en place pour contrôler l'installation du logiciel sur les systèmes en exploitation.

Préconisations de mise en œuvre

Pour réduire le plus possible le risque d'altération des systèmes en exploitation, il convient de tenir compte des lignes directrices suivantes, afin de contrôler les changements:

a) il convient que la mise à jour du logiciel en exploitation, des applications et des bibliothèques de programmes soit réalisée uniquement par des administrateurs qualifiés, après accord de la direction (voir 12.4.3);

b) il convient que les systèmes en exploitation contiennent uniquement du code exécutable approuvé et non du code en développement ou des compilateurs;

c) il convient de mettre en œuvre les applications et le logiciel d'exploitation seulement au terme d'une série d'essais très complète et ayant donné des résultats satisfaisants: essais portant sur l'aptitude à l'emploi, la sécurité, les effets sur les autres systèmes et la convivialité, à réaliser sur des systèmes séparés (voir également 10.1.4); il convient de vérifier que toutes les bibliothèques de programmes ont été mises à jour;

d) il convient d'utiliser un système de contrôle de la configuration afin de conserver le contrôle de tous les logiciels mis en œuvre, ainsi que de la documentation système;

e) il convient de mettre en place une stratégie de retour en arrière avant d'appliquer des modifications;

f) il convient de tenir à jour un rapport d'audit de toutes les mises à jour réalisées sur les bibliothèques de programmes en exploitation;

g) il convient de conserver les versions antérieures du logiciel d'application dans le cadre d'un plan de secours;

h) il convient d'archiver les versions antérieures du logiciel, ainsi que l'ensemble des informations, paramètres, procédures, détails de configuration et logiciels complémentaires associés pendant toute la durée d'archivage des données.

Pour les logiciels fournis par l'éditeur et installés sur les systèmes en exploitation, il convient d'assurer une maintenance permettant de bénéficier de l'assistance technique de l'éditeur. Au fil du temps, les éditeurs de logiciels cessent de fournir une assistance technique pour les anciennes versions. Il convient que l'organisme tienne compte des risques associés à l'utilisation de logiciels dont la maintenance n'est pas prise en charge par l'éditeur.

Il convient que toute décision d'acquérir une nouvelle version tienne compte des exigences métier à l'origine du changement, ainsi que des questions de sécurité liées à la nouvelle version, à savoir l'introduction d'une nouvelle fonction de sécurité ou le nombre et la gravité des problèmes de sécurité liés à cette version. Il convient d'appliquer des correctifs logiciels permettant de supprimer ou de réduire les failles de sécurité (voir également 12.6.1).

Il convient d'accorder l'accès physique ou logique aux éditeurs uniquement pour les besoins de l'assistance technique, de manière ponctuelle, après accord de la direction. Il convient de surveiller les activités du personnel intervenant pour le compte de l'éditeur.

Les logiciels peuvent dépendre de logiciels et modules fournis par un tiers qu'il convient de surveiller et de contrôler, afin d'éviter tout changement non autorisé susceptible d'introduire des failles de sécurité.

Informations supplémentaires

Il convient de mettre à niveau les systèmes d'exploitation uniquement si nécessaire, par exemple si la version actuelle du système d'exploitation ne satisfait plus aux exigences métier. Il convient de ne pas mettre le système à niveau sur le seul motif qu'une nouvelle version du système d'exploitation est disponible. Les nouvelles versions des systèmes d'exploitation peuvent être moins sûres, moins stables et moins bien reconnues par les systèmes actuels.

12.4.2 Protection des données système d'essai

Mesure

Il convient que les données d'essai soient sélectionnées avec soin, protégées et contrôlées.

Directives de mise en œuvre

Dans le cadre d'essais, il convient d'éviter d'utiliser les bases de données fonctionnelles contenant des informations personnelles ou toute autre information sensible. Si une information personnelle ou toute autre information sensible est utilisée dans le cadre d'essais, il convient de supprimer tous les détails et contenus sensibles ou de les modifier de manière à les rendre anonymes avant de les utiliser. Lorsque des données d'exploitation sont utilisées pour les besoins d'un essai, il convient d'appliquer les lignes directrices suivantes afin de les protéger:

a) il convient que les procédures de contrôle d'accès, qui s'appliquent aux applications en exploitation, s'appliquent également aux applications d'essai;

b) il convient d'obtenir une autorisation séparée chaque fois qu'une information d'exploitation est copiée dans une application d'essai;

c) il convient d'effacer les informations d'exploitation d'une application d'essai immédiatement après la fin des essais;

d) il convient de journaliser toute reproduction et utilisation des informations d'exploitation, afin de créer une trace d'audit.

Informations supplémentaires

Les essais de recette et les essais système nécessitent généralement d'importants volumes de données d'essai qui soient le plus représentatives possible des données d'exploitation.

12.4.3 Contrôle d'accès au code source du programme

Mesure

Il convient de restreindre l'accès au code source du programme.

Directives de mise en œuvre

Il convient d'exercer un contrôle strict concernant l'accès au code source des programmes et aux éléments associés (tels que les exigences de conception, les spécifications, les programmes de vérification et de validation), afin d'empêcher l'introduction d'une fonction non autorisée et d'éviter toute modification involontaire. Pour le code source du programme, ce contrôle peut prendre la forme d'un stockage centralisé, de préférence dans les bibliothèques de programmes sources. Il convient de tenir compte des lignes directrices suivantes (voir également Article 11) afin de contrôler l'accès aux bibliothèques de programmes et de réduire les risques d'altération des programmes informatiques:

a) lorsque cela est possible, il convient que les bibliothèques de programmes ne soient pas stockées sur les systèmes en exploitation;

b) il convient que le code source du programme et les bibliothèques de programmes soient gérés conformément aux procédures établies;

c) il convient que le personnel chargé de l'assistance technique ne dispose pas d'un accès illimité aux bibliothèques de programmes;

d) il convient que la mise à jour des bibliothèques de programmes source et des éléments associés ainsi que la délivrance des programmes source aux programmeurs soient réalisées uniquement après accord;

e) il convient de stocker les listings de programmes dans un environnement sécurisé (voir 10.7.4);

f) il convient de tenir à jour un rapport d'audit de tous les accès aux bibliothèques de programmes;

g) il convient de soumettre les processus de maintenance et de reproduction des bibliothèques de programmes à des procédures strictes de contrôle des modifications (voir 12.5.1).

Informations supplémentaires

Le code source du programme est élaboré par les programmeurs; il est compilé (et lié) en vue de créer des exécutables. Certains langages de programmation ne font pas la distinction formelle entre le code source et les exécutables car les exécutables sont créés au moment où ils sont activés.

Pour un complément d'information sur la gestion de la configuration et le cycle de vie des logiciels, voir l'ISO 10007 et l'ISO/CEI 12207.

12.5 Sécurité en matière de développement et d'assistance technique

Objectif: garantir la sécurité du logiciel et des informations d'application.

Il convient de mettre en place des mesures strictes pour l'environnement projet et l'environnement support.

Il convient que les responsables en charge des applications soient également chargées de la sécurité de l'environnement projet ou support. Il convient que ces responsables soient chargés du réexamen de toutes les propositions de modification du système afin de s'assurer que leur mise en œuvre ne compromet pas la sécurité du système ou de l'environnement d'exploitation.

12.5.1 Procédures de contrôle des modifications

Mesure

Il convient de contrôler la mise en œuvre des modifications par le biais de procédures formelles.

Préconisations de mise en œuvre

Il convient de documenter et de mettre en vigueur des procédures formelles de contrôle des modifications afin de réduire le plus possible l'altération des systèmes d'information. Il convient que l'introduction de nouveaux systèmes et les changements de grande ampleur apportés aux systèmes existants suivent une procédure formelle de documentation, de spécification, de mise à l'essai, de contrôle qualité et de mise en œuvre.

Il convient que ce processus prévoie une appréciation du risque, une analyse des impacts du changement et une spécification des mesures de sécurité requises. Il convient que ce processus garantisse la non-compromission des procédures de sécurité et de contrôle. Il convient également qu'il limite l'accès accordé aux programmeurs chargés de l'assistance aux seules parties du système sur lesquelles ils doivent intervenir et qu'il garantisse l'obtention d'un accord formel avant tout changement.

Le cas échéant, il convient d'intégrer les procédures de contrôle des modifications, au niveau des applications et au niveau du système en exploitation (voir également 10.1.2). Dans le cadre des procédures de changement, il convient de tenir la conduite suivante:

a) tenir à jour un enregistrement des niveaux d'autorisation accordés;

b) veiller à ce que les propositions de changements émanent d'utilisateurs habilités;

c) réexaminer les procédures de contrôle et de protection de l'intégrité des données afin de s'assurer qu'elles ne seront pas compromises par les changements;

d) identifier tout(e) logiciel, information, élément de base de données et matériel nécessitant une modification;

e) obtenir un accord formel pour les propositions détaillées avant le lancement des travaux;

f) s'assurer que les utilisateurs habilités acceptent les changements avant leur mise en œuvre;

g) veiller à la mise à jour de la documentation système après chaque changement et à l'archivage ou la mise au rebut de l'ancienne documentation;

h) tenir à jour un contrôle de version pour toutes les mises à jour logicielles;

i) tenir à jour une trace d'audit pour toute demande de changement;

j) veiller à ce que la documentation du système d'exploitation (voir 10.1.1) et les procédures utilisateurs soient adaptées en fonction des changements;

k) veiller à programmer la mise en œuvre des changements de manière à ne pas perturber les activités de l'organisme.

Informations supplémentaires

Un changement apporté aux logiciels peut avoir une incidence sur l'environnement en exploitation.

Selon les bonnes pratiques, la mise à l'essai d'un nouveau logiciel doit être réalisée dans un environnement isolé des environnements de production et de développement (voir également 10.1.4). Ce cloisonnement permet de contrôler le nouveau logiciel et d'ajouter une protection supplémentaire pour les informations d'exploitation utilisées dans le cadre d'essais. Il s'agit notamment des correctifs logiciels, des «service packs» (ensembles de modifications provisoires) et d'autres mises à jour. Il convient de ne pas mettre en œuvre les mises à jour automatisées sur des systèmes critiques, car certaines mises à jour sont susceptibles de faire échouer des applications critiques (voir 12.6).

12.5.2 Réexamen technique des applications après modification du système d'exploitation

Mesure

Lorsque des modifications sont apportées aux systèmes d'exploitation, il convient de réexaminer et de soumettre à essai les applications critiques de gestion afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

Préconisations de mise en œuvre

Il convient que ce processus prévoie les actions suivantes:

a) réexaminer les procédures de contrôle d'intégrité des applications afin de s'assurer qu'elles n'ont pas été compromises par les modifications apportées au système d'exploitation;

b) s'assurer que le plan annuel d'assistance et le budget correspondant prévoient des réexamens et essais en cas de modification du système d'exploitation;

c) veiller à ce que les modifications du système d'exploitation soient notifiées en temps opportun, afin que les essais et réexamens appropriés soient réalisés avant la mise en œuvre de ces modifications;

d) veiller à ce que les plans de continuité de l'activité soient modifiés en conséquence (voir Article 14).

Il convient qu'une personne ou qu'un groupe spécifique de personnes soi(en)t chargée(s) de surveiller les vulnérabilités et la publication des correctifs (voir 12.6).

12.5.3 Restrictions relatives à la modification des progiciels

Mesure

Il convient de ne pas encourager la modification des progiciels et de se limiter aux changements nécessaires. Il convient également d'exercer un contrôle strict sur ces modifications.

Préconisations de mise en œuvre

Dans la mesure du possible, il convient de ne pas apporter de modifications aux progiciels fournis par l'éditeur. Lorsqu'une modification du progiciel est nécessaire, il convient de tenir compte des points suivants:

a) le risque de compromettre les commandes intégrées et les processus de vérification de l'intégrité;

b) est-il nécessaire d'obtenir le consentement de l'éditeur ?

c) la possibilité d'obtenir les modifications souhaitées auprès de l'éditeur, sous la forme de mises à jour de programme classiques;

d) lorsque l'organisme apporte des modifications au logiciel, il devient responsable de la maintenance de celui-ci: quelles en sont les conséquences ?

Lorsqu'une modification est nécessaire, il convient de conserver le logiciel original et d'appliquer cette modification sur une copie clairement identifiée. Il convient d'appliquer une politique de gestion des mises à jour afin que tous les logiciels autorisés bénéficient des versions et des correctifs logiciels les plus récents (voir 12.6). Il convient de soumettre à essai et de documenter tous les changements apportés afin de pouvoir les réappliquer aux versions ultérieures, le cas échéant. S'il y a lieu, les modifications peuvent être évaluées et validées par un organisme indépendant.

12.5.4 Fuite d'informations

Mesure

Il convient d'empêcher toute possibilité de fuite d'informations.

Préconisations de mise en œuvre

Pour limiter le risque de fuite d'informations via des canaux cachés, il convient de procéder comme suit:

a) analyser les supports et communications sortants pour détecter d'éventuelles informations cachées;

b) masquer et moduler le comportement des systèmes et des communications afin de réduire les risques de voir les tiers déduire des informations à partir de l'analyse d'un tel comportement;

c) utiliser des systèmes et logiciels considérés comme offrant un haut niveau d'intégrité, par exemple des produits évalués (voir l'ISO/CEI 15408);

d) assurer une surveillance régulière des activités du personnel et des opérations système, lorsque les règlements ou législations en vigueur le permettent;

e) surveiller l'emploi des ressource stockées sur les systèmes informatiques.

Informations supplémentaires

Les canaux cachés sont des chemins qui n'ont pas vocation à acheminer des flux d'informations, mais qui pourtant existent dans un système ou un réseau. Par exemple, il est possible d'émettre un signal de manière clandestine en manipulant des bits transmis dans des paquets de protocoles de communication. De par leur nature, il est difficile voire impossible de supprimer tous les canaux cachés potentiels. Toutefois, ces canaux étant souvent exploités par du code cheval de Troie (voir également 10.4.1), l'utilisation de mesures de protection contre ce code permet de réduire le risque associé aux canaux cachés.

Il est également possible de se prémunir contre les canaux cachés en interdisant les accès non autorisés au réseau (11.4) et en mettant en place des politiques et procédures visant à dissuader le personnel de faire un mauvais usage des services d'information (15.1.5).

12.5.5 Externalisation du développement logiciel

Mesure

Il convient que l'organisme encadre et contrôle le développement logiciel externalisé.

Préconisations de mise en œuvre

Lorsque le développement logiciel est sous-traité, il convient de tenir compte des points suivants:

a) accords de licence, propriété du code et droits de propriété intellectuelle (voir 15.1.2);

b) certification de la qualité et précision des travaux réalisés;

c) dispositions relatives au séquestre, en cas de manquement du tiers;

d) droits d'accès permettant d'auditer la qualité et précision des travaux réalisés;

e) exigences contractuelles relatives à la qualité et au niveau de sécurité du code;

f) essais préalables à l'installation, visant à détecter les codes malveillants éventuels et le code cheval de Troie.

12.6 Gestion des vulnérabilités techniques

Objectif: réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication.

Il convient de mettre en œuvre une gestion des vulnérabilités techniques de manière efficace, systématique et répétable et d'effectuer des mesurages pour confirmer son efficacité. Il s'agit ici des systèmes d'exploitation et de toute autre application en cours d'utilisation.

12.6.1 Mesure relative aux vulnérabilités techniques

Mesure

Il convient d'être informé en temps voulu de toute vulnérabilité technique des systèmes d'information en exploitation, d'évaluer l'exposition de l'organisme audites vulnérabilités et d'entreprendre les actions appropriées pour traiter le risque associé.

Préconisations de mise en œuvre

Pour une gestion efficace des vulnérabilités techniques, il est impératif de disposer d'un inventaire des biens, exhaustif et à jour (voir 7.1). Les informations spécifiques nécessaires à la gestion des vulnérabilités techniques sont les suivantes: nom de l'éditeur du logiciel, numéros de version, état de déploiement (par exemple quel logiciel est installé sur quels systèmes) et nom de la (des) personne(s) responsable(s) du logiciel au sein de l'organisme.

Dès l'identification de vulnérabilités techniques potentielles, il convient d'engager l'action appropriée, dans les meilleurs délais. Il convient d'appliquer les recommandations suivantes pour établir un processus de gestion des vulnérabilités techniques:

a) il convient que l'organisme définisse et établisse les rôles et responsabilités associés à la gestion des vulnérabilités techniques, notamment la veille en matière de vulnérabilités, l'appréciation du risque, l'application de correctifs logiciels, le suivi des biens, ainsi que toute responsabilité de coordination requise;

b) il convient de déterminer les ressources d'information permettant d'identifier les vulnérabilités techniques et de sensibiliser les intervenants sur ces vulnérabilités, pour les logiciels et les autres technologies (sur la base de l'inventaire des biens, voir 7.1.1); il convient de mettre à jour ces ressources d'information sur la base des changements effectués dans l'inventaire ou lorsque des ressources nouvelles ou utiles sont découvertes;

c) il convient de définir un délai de réaction aux notifications relatives à d'éventuelles vulnérabilités techniques;

d) lorsqu'une vulnérabilité technique potentielle est identifiée, il convient que l'organisme détermine les risques associés et les actions à entreprendre; cela peut consister à installer un correctif logiciel sur les systèmes vulnérables et/ou à appliquer d'autres mesures;

e) suivant l'urgence de l'action corrective, il convient d'appliquer soit des mesures de gestion des modifications (voir 12.5.1) soit des procédures de gestion des incidents liés à la sécurité de l'information (voir 13.2);

f) si un correctif logiciel est disponible, il convient d'évaluer les risques associés à l'installation de ce correctif (en comparant les risques découlant des vulnérabilités et les risques associés à l'installation du correctif);

g) il convient d'évaluer et de soumettre à essai les correctifs avant de les installer afin de vérifier leur efficacité et de s'assurer qu'ils n'entraînent pas d'effets secondaires inacceptables; si aucun correctif logiciel n'est disponible, il convient d'envisager d'autres mesures, telles que les suivantes:

   1) désactivation des services ou des fonctions liés aux vulnérabilités;

   2) adaptation ou ajout de contrôles d'accès, par exemple des pare-feu, aux limites du réseau (voir 11.4.5);

   3) renforcement du dispositif de surveillance visant à détecter ou empêcher les attaques;

   4) renforcement de la politique de sensibilisation sur les vulnérabilités;

h) il convient de conserver un rapport d'audit pour toutes les procédures mises en œuvre;

i) il convient de surveiller et d'évaluer à intervalles réguliers le processus de gestion des vulnérabilités techniques afin de garantir son efficacité et son efficacité;

j) il convient de traiter en priorité les systèmes à haut risque.

Informations supplémentaires

Le bon fonctionnement du processus de gestion des vulnérabilités techniques est une question critique pour de nombreux organismes. C'est pourquoi, il convient de mettre en place une surveillance de ce processus. Il est essentiel d'établir un inventaire précis pour garantir la détection des vulnérabilités techniques potentielles.

La gestion des vulnérabilités techniques peut être considérée comme une sous-fonction de la gestion des modifications et peut, de ce fait, bénéficier des mêmes processus et procédures (voir 10.1.2 et 12.5.1).

Les éditeurs étant soumis à d'importantes pressions concernant les délais de publication des correctifs, il peut arriver qu'un correctif ne traite pas le problème de manière adéquate et introduise un effet secondaire indésirable. Dans certains cas, il peut être difficile de désinstaller un correctif une fois qu'il a été appliqué.

S'il n'est pas possible de soumettre le correctif à essai, par exemple pour des raisons de coût ou par manque de ressources, un délai peut être envisagé afin d'évaluer les risques associés, sur la base de l'expérience des autres utilisateurs.

13 Gestion des incidents liés à la sécurité de l'information

13.1 Signalement des événements et des failles liés à la sécurité de l'information

Objectif: garantir que le mode de notification des événements et failles liés à la sécurité de l'information permette la mise en œuvre d'une action corrective, dans les meilleurs délais.

Il convient de mettre en place des procédures formelles de remontée d'information et de signalement progressif. Il convient de sensibiliser tous les salariés, contractants et utilisateurs tiers aux procédures de signalement des différents types d'événements et de failles susceptibles d'avoir une incidence sur la sécurité des biens de l'organisme. Il convient qu'ils signalent le plus rapidement possible tout événement ou faille de sécurité à l'interlocuteur désigné.

13.1.1 Signalement des événements liés à la sécurité de l'information

Mesure

Il convient de signaler, dans les meilleurs délais, les événements liés à la sécurité de l'information, par les voies hiérarchiques appropriées.

Préconisations de mise en œuvre

Il convient d'établir une procédure formelle de signalement, ainsi qu'une procédure de remontée d'informations et de réponse en cas de détection d'un incident lié à la sécurité de l'information, définissant les mesures à prendre à la réception d'un rapport signalant un tel événement. Il convient de désigner un responsable à contacter pour le signalement des événements liés à la sécurité de l'information. Il convient que ce responsable à contacter soit connu de tous au sein de l'organisme, qu'il soit toujours disponible et mette en œuvre une action adéquate et rapide.

Il convient d'informer tous les salariés, contractants et utilisateurs tiers de leur obligation de signaler tout événement lié à la sécurité de l'information dans les meilleurs délais. Il convient de les informer de l'existence d'une procédure de signalement des événements liés à la sécurité de l'information et d'un responsable à contacter. Il convient que les procédures de signalement prévoient ce qui suit:

a) des processus de retour d'information adéquats, afin de communiquer les détails de la résolution du problème aux personnes ayant signalé un événement;

b) des formulaires, pour faciliter le signalement, récapitulant toutes les actions à mettre en œuvre lorsqu'un événement lié à la sécurité de l'information est détecté;

c) le comportement du personnel en cas d'événements liés à la sécurité de l'information, à savoir:

   1) noter immédiatement tous les détails importants (par exemple le type de non-conformité ou de violation, le dysfonctionnement observé, les messages affichés à l'écran, un comportement bizarre);

   2) ne pas prendre d'initiative personnelle et signaler immédiatement le problème au responsable à contacter;

d) un processus disciplinaire formel pour les salariés, les contractants ou les utilisateurs tiers ayant enfreint les règles de sécurité.

Dans les environnements à haut risque, l'installation d'une alarme sous contrainte[3)] peut être envisagée, pour permettre à une personne se trouvant sous la contrainte de quelqu'un de donner l'alarme. Il convient que les procédures de réponse à une alarme de contrainte individuelle soient adaptées à la situation.

Informations supplémentaires

Exemples d'événements et incidents liés à la sécurité de l'information:

a) la perte de service, de matériels ou d'équipements;

b) un dysfonctionnement ou une surcharge du système;

c) une erreur humaine;

d) le non-respect des politiques ou des recommandations;

e) une violation des dispositions relatives à la sécurité physique;

---

3) Une alarme sous contrainte permet à une personne se trouvant sous une contrainte quelconque de signaler discrètement sa situation.

f) un changement non contrôlé apporté au système;

g) un dysfonctionnement logiciel ou matériel;

h) une violation d'accès.

Dans le cadre d'un programme de sensibilisation des utilisateurs (voir 8.2.2) et dans le respect des exigences de confidentialité, il est possible d'utiliser les incidents liés à la sécurité de l'information afin de présenter les situations susceptibles de se produire, le mode de traitement de ce type d'incidents et les procédures à mettre en place afin d'éviter leur réapparition. Pour répondre correctement aux événements et incidents liés à la sécurité de l'information, une intervention rapide peut s'avérer nécessaire de recueillir des preuves le plus tôt possible après la survenue de l'incident (voir 13.2.3).

Les éventuels dysfonctionnements ou autres comportements anormaux du système peuvent révéler une attaque ou une brèche dans la sécurité et il convient par conséquent de signaler ces phénomènes comme des événements liés à la sécurité de l'information.

Pour un complément d'information sur le signalement des événements liés à la sécurité de l'information et la gestion des incidents liés à la sécurité de l'information, voir l'ISO/CEI TR 18044.

13.1.2 Signalement des failles de sécurité

Mesure

Il convient de demander à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

Préconisations de mise en œuvre

Il convient que tous les salariés, contractants et utilisateurs tiers signalent ce type de problème à leur responsable direct ou à leur prestataire de service, dans les meilleurs délais, afin d'éviter tout incident lié à la sécurité de l'information. Il convient que le mécanisme de signalement soit le plus simple, accessible et disponible possible. Il convient de recommander à ces personnes de ne tenter d'apporter la preuve de failles de sécurité soupçonnées en aucune circonstance.

Informations supplémentaires

Il convient de recommander aux salariés, contractants et utilisateurs tiers de ne pas tenter de démontrer l'existence d'éventuelles failles de sécurité. Une telle tentative pourrait être interprétée comme un mauvais usage potentiel du système et endommager le système ou le service d'information. La personne qui prendrait une telle initiative s'exposerait à des poursuites judiciaires.

13.2 Gestion des améliorations et incidents liés à la sécurité de l'information

Objectif: garantir la mise en place d'une politique cohérente et efficace pour la gestion des incidents liés à la sécurité de l'information.

Il convient de définir des responsabilités et des procédures permettant une gestion efficace des événements et failles de sécurité après leur signalement. Il convient d'appliquer un processus d'amélioration continue pour la surveillance, l'évaluation et la gestion globale des incidents liés à la sécurité de l'information, ainsi que pour les actions correctives mises en œuvre.

Lorsque cela s'avère nécessaire, il convient de recueillir des preuves afin de satisfaire aux exigences légales.

13.2.1 Responsabilités et procédures

Mesure

Il convient d'établir des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.

Préconisations de mise en œuvre

Outre le signalement des événements et failles liés à la sécurité de l'information (voir également 13.1), il convient de mettre en place une surveillance des systèmes, des alertes et des vulnérabilités (10.10.2) afin de détecter les incidents liés à la sécurité de l'information. Dans le cadre des procédures de gestion des incidents liés à la sécurité de l'information, il convient de tenir compte des directives suivantes:

a) il convient d'établir des procédures permettant de gérer les différents types d'incidents liés à la sécurité de l'information, notamment les aspects suivants:

   1) défaillances du système d'information et perte du service;

   2) codes malveillants (voir 10.4.1);

   3) refus de service;

   4) erreurs dues à des données liées à l'activité incomplètes ou inexactes;

   5) non-respect des exigences de confidentialité et d'intégrité;

   6) mauvais usage des systèmes d'information.

b) outre les plans de secours habituels (voir 14.1.3), il convient que les procédures couvrent également les aspects suivants (voir également 13.2.2):

   1) analyse et identification de la cause de l'incident;

   2) confinement;

   3) planification et mise en œuvre des actions correctives destinées à empêcher les récurrences, si nécessaire;

   4) prise de contact avec les personnes concernées par l'incident;

   5) signalement de l'action à l'autorité compétente;

c) il convient de recueillir et de stocker en lieu sûr les traces d'audit et autres éléments de preuves (voir 13.2.3), s'il y a lieu, pour les besoins suivants:

   1) analyse du problème en interne;

   2) utilisation de preuves scientifiques liées à une violation potentielle de clauses contractuelles ou d'exigences réglementaires, ou dans le cas de poursuites civiles ou pénales, par exemple des cas tombant sous le coup de la législation relative à la protection des données ou au mauvais usage des biens informatiques;

   3) négociation d'une compensation auprès de fournisseurs de logiciels ou de services;

d) il convient de contrôler avec soin les actions visant à remédier aux brèches dans la sécurité et aux défaillances du système, dans le cadre d'une procédure formelle; il convient que ces procédures garantissent ce qui suit:

   1) seul le personnel clairement identifié et habilité est autorisé à accéder aux systèmes et données en exploitation (voir également 6.2 pour les accès externes);

2) toutes les actions d'urgence sont documentées en détail;

3) les actions d'urgence sont signalées à la direction et réexaminées de manière méthodique;

4) l'intégrité des systèmes et mesures de gestion est confirmée dans les meilleurs délais.

Il convient que les objectifs de la gestion des incidents liés à la sécurité de l'information fassent l'objet d'un accord avec la direction. Il convient également de s'assurer que les personnes responsables de la gestion des incidents liés à la sécurité de l'information connaissent les priorités de l'organisme dans ce domaine.

Informations supplémentaires

Les incidents liés à la sécurité de l'information peuvent dépasser les frontières de l'organisme et du pays. Pour traiter ce type d'incidents, il est de plus en plus nécessaire de coordonner les réponses et de partager les informations relatives à ces incidents avec les autres organismes s'il y a lieu.

13.2.2 Exploitation des incidents liés à la sécurité de l'information déjà survenus

Mesure

Il convient de mettre en place des mécanismes permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume et les coûts associés.

Préconisations de mise en œuvre

Il convient de réinvestir les informations recueillies lors de la résolution d'incidents liés à la sécurité de l'information pour identifier les incidents récurrents ou ayant un fort impact.

Informations supplémentaires

L'évaluation d'incidents liés à la sécurité de l'information peut faire apparaître la nécessité d'améliorer les mesures existantes ou d'en créer de nouvelles, afin de limiter la fréquence des futurs incidents ainsi que les dommages et les coûts associés, ou afin d'intégrer ces mesures dans le processus de réexamen de la politique de sécurité (voir 5.1.2).

13.2.3 Collecte de preuves

Mesure

Lorsqu'une action en justice civile ou pénale est engagée contre une personne physique ou un organisme, à la suite d'un incident lié à la sécurité de l'information, il convient de recueillir, conserver et présenter les informations conformément aux dispositions légales relatives à la présentation de preuves régissant la ou les juridiction(s) compétente(s).

Préconisations de mise en œuvre

Il convient de mettre au point et d'appliquer des procédures internes lors de la collecte et la présentation des preuves dans le cadre d'une action disciplinaire au sein d'un organisme.

En général, les règles s'appliquant aux preuves sont les suivantes:

a) l'admissibilité de la preuve: les preuves peuvent-elles être présentées devant un tribunal ?

b) la valeur probante: la qualité et l'exhaustivité d'une preuve.

Pour obtenir l'admissibilité de la preuve, il convient que l'organisme garantisse la conformité des systèmes d'information avec une norme ou un code de bonnes pratiques publié(e) définissant la production des preuves admissibles.

La preuve doit également être conforme aux exigences applicables en matière de valeur probante. Pour obtenir une valeur probante, il convient de démontrer la qualité et l'exhaustivité des mesures mises en œuvre pour protéger les éléments de preuve de manière efficace et cohérente. Il convient également de démontrer, par le biais d'une solide chaîne de preuves, que les preuves à récupérer ont été stockées et traitées (preuve du processus de contrôle. En général, il est possible d'établir une telle chaîne de preuves dans les conditions suivantes:

a) pour les documents papier: l'original est conservé en lieu sûr et accompagné d'un enregistrement identifiant la personne qui a trouvé le document, précisant le moment et les éventuels témoins de la découverte; il convient de réaliser une enquête pour s'assurer de l'authenticité des originaux;

b) pour les informations stockées sur un support informatique: pour garantir leur disponibilité, il convient de réaliser des images du support ou des copies (suivant les exigences applicables) des informations stockées sur un support mobile, un disque dur ou un support-mémoire; il convient de surveiller le processus de reproduction et de conserver le journal de toutes les opérations réalisées; il convient de conserver en lieu sûr le support et le journal originaux (si cela s'avère impossible, au moins une image du support ou une copie).

Il convient que les travaux des experts scientifiques soient réalisés uniquement sur des copies des éléments de preuve. Il convient de protéger l'intégrité des éléments de preuve. Il convient que la reproduction de tout élément de preuve soit encadrée par une personne de confiance. Il convient de journaliser les éléments suivants: quelles informations ont été reproduites, quand cette opération a eu lieu, par qui a-t-elle été réalisée, quels outils et programmes ont été utilisés.

Informations supplémentaires

À la première détection d'un événement lié à la sécurité de l'information, il n'est pas toujours possible de prévoir si l'événement fera l'objet d'une action en justice. Les preuves potentielles risquent donc d'être détruites, volontairement ou non, avant que la gravité de l'incident ne soit avérée. Il est souhaitable de consulter un avocat ou la police rapidement, en vue d'une éventuelle action en justice, afin de recueillir les conseils relatifs à la preuve.

La preuve peut dépasser les limites de l'organisme et/ou les frontières juridictionnelles. Dans ce cas, il convient de s'assurer que l'organisme est habilité à recueillir les informations devant servir de preuve. Il convient de tenir compte des exigences des diverses juridictions afin d'optimiser l'admissibilité de la preuve auprès des juridictions compétentes.

14 Gestion du plan de continuité de l'activité

14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité

Objectif: neutraliser les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.

Il convient de mettre en œuvre un processus de gestion du plan de continuité de l'activité visant à réduire le plus possible l'impact sur l'organisme et à récupérer les actifs informationnels perdus (notamment à la suite de catastrophes naturelles, d'accidents, de pannes de matériel et d'actes délibérés). Des mesures préventives et correctives sont prises dans le but d'atteindre un niveau de récupération suffisant. Il convient d'identifier les processus métier cruciaux et d'associer les exigences de gestion de la sécurité de l'information en matière de continuité de l'activité aux autres exigences liées à la continuité affectant des domaines tels que l'exploitation, l'affectation des effectifs, le matériel, le transport et les équipements.

Il convient de soumettre les conséquences des sinistres, des défaillances de sécurité, de la perte de service et de la disponibilité de service à une analyse de l'impact sur l'activité de l'organisme. Il convient d'élaborer et de mettre en œuvre des plans de continuité de l'activité visant à garantir une reprise des opérations essentielles dans les meilleurs délais. Il convient que la sécurité de l'information fasse partie intégrante du processus de continuité de l'activité dans son ensemble et des autres processus de gestion inhérents à l'organisme.

Il convient que la gestion du plan de continuité de l'activité prévoie, outre le processus général d'appréciation du risque, des mesures destinées à identifier et à réduire les risques, limite les conséquences d'incidents dommageables et garantisse l'accès aisé à l'information requise dans le cadre du processus métier.

14.1.1 Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité

Mesure

Il convient d'élaborer et de gérer un processus de continuité de l'activité dans l'ensemble de l'organisme qui satisfait aux exigences en matière de sécurité de l'information requises pour la continuité de l'activité de l'organisme.

Préconisations de mise en œuvre

Il convient que ce processus regroupe les éléments clé suivants du plan de continuité de l'activité:

a) comprendre les risques auxquels l'organisme doit faire face en termes de probabilité et d'impact sur le temps, y compris une identification et une hiérarchisation des processus métier cruciaux (voir 14.1.2);

b) identifier tous les biens en jeu dans les processus métier cruciaux (voir 7.1.1);

c) analyser l'impact probable des interruptions causées par des incidents liés à la sécurité de l'information sur les activités de l'organisme (il est important de trouver des solutions aux incidents ayant un impact plus faible et des solutions aux incidents plus lourds pouvant nuire à la rentabilité de l'organisme) et définir le rôle des moyens de traitement de l'information dans l'activité de l'organisme.

d) envisager la souscription d'une assurance adaptée pouvant faire partie du processus global de continuité de l'activité et de la gestion du risque opérationnel;

e) définir et envisager la mise en œuvre de mesures préventives et atténuantes supplémentaires;

f) identifier les ressources financières, d'organisation, techniques et environnementales suffisantes pour satisfaire aux exigences définies en matière de sécurité de l'information;

g) assurer la sécurité du personnel et garantir la protection des moyens de traitement de l'information et des biens matériels de l'organisme;

h) préparer et documenter les plans de continuité de l'activité satisfaisant aux exigences en matière de sécurité de l'information conformément à la stratégie de continuité de l'activité définie (voir 14.1.3);

i) soumettre à essai et mettre à jour de façon régulière les plans et processus mis en place (voir 14.1.5);

j) veiller à ce que la gestion du plan de continuité de l'activité soit intégrée aux processus et à la structure de l'organisme; il convient d'attribuer la responsabilité du processus de gestion du plan de continuité de l'activité au niveau approprié de l'organisme (voir 6.1.1).

14.1.2 Continuité de l'activité et appréciation du risque

Mesure

Il convient d'identifier les événements pouvant être à l'origine d'interruptions des processus métier tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information.

Préconisations de mise en œuvre

Il convient que les aspects de la sécurité de l'information en matière de continuité de l'activité reposent sur des événements d'identification (ou une suite d'événements) pouvant être à l'origine d'interruptions des processus métier de l'organisme telles qu'une panne de matériel, une erreur humaine, un vol, un incendie, une catastrophe naturelle et des attaques terroristes. Il convient ensuite de procéder à une appréciation du risque afin de déterminer la probabilité et l'impact de telles interruptions en termes de temps, d'ampleur des sinistres et de période de récupération.

Il convient de mener à bien l'appréciation du risque en matière de continuité de l'activité conjointement avec les propriétaires des processus et des ressources liés à l'activité de l'organisme. Il convient que cette appréciation prenne en compte l'ensemble des processus métier, et ne se limite pas aux moyens de traitement de l'information mais englobe les résultats spécifiques à la sécurité de l'information. Il est important d'associer les différents aspects du risque afin d'obtenir une image complète des exigences de l'organisme en matière de continuité de l'activité. Il convient que l'appréciation identifie, quantifie et hiérarchise les risques en fonction des critères et des objectifs significatifs pour l'organisme, y compris les ressources cruciales, les impacts des interruptions, les temps d'indisponibilité et les priorités de récupération.

En fonction des résultats de l'appréciation du risque, il convient d'élaborer une stratégie de continuité de l'activité visant à déterminer l'approche globale de la continuité de l'activité. Une fois la stratégie créée, il convient qu'elle soit approuvée par la direction et qu'un plan soit créé et également approuvé pour mettre en œuvre cette stratégie.

14.1.3 Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information

Mesure

Il convient d'élaborer et de mettre en œuvre des plans destinés à maintenir ou à restaurer l'exploitation et à assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.

Préconisations de mise en œuvre

Il convient de prendre en compte les éléments suivants par le biais de la planification de la continuité de l'activité:

a) l'identification et l'acceptation de l'ensemble des responsabilités et des procédures liées à la continuité de l'activité;

b) l'identification du niveau de perte d'informations et de services acceptable;

c) la mise en œuvre des procédures destinées à permettre la récupération et la restauration des exploitations liées à l'activité de l'organisme et la disponibilité des informations dans les délais requis; une attention particulière doit être portée à l'appréciation des dépendances entre les activités internes et externes et les contrats conclus;

d) les procédures d'exploitation à mettre en place lors de la récupération et de la restauration;

e) la documentation des procédures et processus convenus;

f) la formation adaptée du personnel aux procédures et processus définis, y compris la gestion de crise;

g) la mise à l'essai et la mise à jour des plans.

Il convient que le processus de planification s'attache principalement aux objectifs requis liés à l'activité de l'organisme, par exemple la restauration des services de communication spécifiques avec les clients dans un délai acceptable. Il convient d'identifier les services et ressources visant cet objectif, y compris l'affectation des effectifs, les ressources non affectées au traitement de l'information ainsi que les dispositions de repli pour les moyens de traitement de l'information. Ces dispositions de repli peuvent inclure des accords avec des tiers, tels que les accords de réciprocité ou de services d'abonnement commercial.

Il convient que le plan de continuité de l'activité prenne en compte les vulnérabilités de l'organisme; en conséquence, il peut contenir des informations sensibles nécessitant une protection appropriée. Il convient de placer les sauvegardes de copies du plan de continuité de l'activité dans un emplacement distant, c'est-à-dire à une distance suffisante pour échapper aux dégâts d'une catastrophe sur le site principal. Il convient que la direction garantisse la mise à jour des copies du plan de continuité de l'activité et leur protection à un niveau identique à celui appliqué sur le site principal. Il convient également de stocker le matériel supplémentaire nécessaire à l'exécution du plan de continuité dans un emplacement distant.

Si des emplacements temporaires alternatifs sont utilisés, il convient que le niveau des mesures de sécurité mises en œuvre dans ces emplacements soit équivalent à celui du site principal.

Informations supplémentaires

Il convient de souligner que les plans et activités de la gestion de crise [voir 14.1.3 f)] peuvent différer du plan de gestion de continuité de l'activité; une crise émergente peut par exemple être traitée par les procédures de gestion habituelles.

14.1.4 Cadre de la planification de la continuité de l'activité

Mesure

Il convient gérer un cadre unique pour les plans de continuité de l'activité afin de garantir la cohérence de l'ensemble des plans, de satisfaire de manière constante aux exigences en matière de sécurité de l'information et d'identifier les priorités en matière de mise à l'essai et de maintenance.

Préconisations de mise en œuvre

Il convient que chaque plan de continuité de l'activité décrive l'approche retenue dans ce domaine; l'objectif pouvant être de garantir la disponibilité et la sécurité des informations ou du système d'information. Il convient que chaque plan spécifie également la procédure de remontée d'informations et les conditions de son activation ainsi que les personnes responsables de l'exécution de chaque élément du plan. Lorsque de nouvelles exigences sont identifiées, il convient de modifier, le cas échéant, toute procédure d'urgence existante comme les plans d'évacuation ou les dispositions de repli. Il convient d'intégrer des procédures au programme de gestion des modifications de l'organisme afin de garantir le traitement toujours approprié de la continuité de l'activité.

En outre, il convient que chaque plan ait un propriétaire propre. Il convient que les procédures d'urgence, plans de repli manuels et plans de reprise soient placés sous la responsabilité des propriétaires des ressources ou des processus fonctionnels appropriés impliqués. Il convient généralement de placer les dispositions de repli pour des services techniques alternatifs comme les moyens de traitement de l'information et de communication sous la responsabilité des prestataires de services.

Il convient que le cadre de la planification de la continuité de l'activité réponde aux exigences identifiées en matière de sécurité de l'information et prenne en compte les éléments suivants:

a) les conditions d'activation des plans décrivant le processus à respecter (par exemple: comment évaluer la situation, les personnes impliquées) avant d'activer chaque plan;

b) les procédures d'urgence décrivant les actions à engager à la suite d'un incident mettant en danger l'activité de l'organisme;

c) les procédures de repli décrivant les actions à engager en vue de déplacer les activités de l'organisme ou les services d'assistance dans des emplacements temporaires alternatifs et de rétablir les processus métier dans les délais requis;

d) les procédures opérationnelles temporaires à mettre en place lors de la récupération et de la restauration;

e) les procédures de reprise décrivant les actions à engager en vue du rétablissement des activités de l'organisme;

f) un calendrier de maintenance spécifiant comment et quand le plan sera soumis à essai et le processus de gestion du plan;

g) les activités relatives à la sensibilisation, la qualification et aux formations dont le but est de faire comprendre les processus de continuité de l'activité et de garantir l'efficacité constante des processus;

h) les responsabilités des personnes indiquant le responsable de l'exécution de chaque élément du plan. Le cas échéant, il convient de désigner des alternatives;

i) les biens et les ressources cruciaux requis pour lancer les procédures d'urgence, de repli et de reprise.

14.1.5 Mise à l'essai, gestion et appréciation constante des plans de continuité de l'activité

Mesure

Il convient de soumettre à essai et de mettre à jour régulièrement les plans de continuité de l'activité afin de s'assurer qu'ils sont actualisés et efficaces.

Préconisations de mise en œuvre

Il convient que les essais du plan de continuité de l'activité garantissent que tous les membres de l'équipe dédiée à la récupération ainsi que les autres membres du personnel concernés sont informés des plans et de leur responsabilité en matière de continuité de l'activité et de sécurité de l'information et connaissent leur rôle au moment du lancement d'un plan.

Il convient que le calendrier des essais pour le(s) plan(s) de continuité de l'activité précise comment et quand il convient de soumettre à essai chaque élément du plan. Il convient que la mise à l'essai de chaque élément du (des) plan(s) soit effectuée de manière fréquente.

Il convient d'employer des techniques multiples dans le but de garantir que le (les) plan(s) fonctionnera (fonctionneront) dans la pratique. Il convient que ces techniques incluent les éléments suivants:

a) une mise à l'essai de scénarios multiples (débat sur les dispositions de récupération en matière d'activité liée à l'organisme à l'aide d'exemples d'interruptions);

b) des simulations (notamment pour la formation des personnes ayant un rôle dans la gestion post-incident/de crise);

c) une mise à l'essai de la récupération technique (garantissant que le système d'information peut être restauré efficacement);

d) une mise à l'essai de la récupération sur un site de substitution (exécution parallèle des processus métier et des opérations de récupération en dehors du site principal);

e) une mise à l'essai des services et équipements du fournisseur (garantissant que les services et les produits d'un fournisseur externe seront conformes à l'engagement pris par contrat);

f) des répétitions complètes (vérifiant que l'organisme, le personnel, le matériel, les équipements et les processus peuvent gérer des situations d'interruptions).

Tout organisme peut appliquer ces techniques. Il convient de les adapter au plan de récupération concerné. Il convient d'archiver les résultats des essais et de prendre des mesures destinées à améliorer les plans, le cas échéant.

Il convient de charger un responsable d'effectuer des réexamens réguliers pour chaque plan de continuité de l'activité. Il convient de procéder à une mise à jour appropriée du plan lorsque l'identification des changements affectant les dispositions liées à l'activité de l'organisme n'est pas répercutée sur les plans de continuité de l'activité. Il convient de garantir, par l'intermédiaire de cette procédure formelle de contrôle des modifications, que les plans mis à jour sont diffusés et améliorés par le biais de réexamens réguliers de l'intégralité du plan.

Il convient d'envisager la mise à jour du plan de continuité de l'activité lors de l'acquisition de nouveau matériel, la mise à niveau des systèmes et les changements affectant les éléments suivants:

a) le personnel;

b) les adresses ou numéros de téléphone;

c) la stratégie propre à l'activité de l'organisme;

d) l'emplacement, les équipements et les ressources;

e) la législation;

f) les contractants, les fournisseurs et les clients principaux;

g) les processus, les processus nouveaux ou ceux qui ne sont plus utilisés;

h) le risque (opérationnel et financier).

15 Conformité

15.1 Conformité avec les exigences légales

Objectif: éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles et des exigences de sécurité.

La conception, l'exploitation, l'utilisation et la gestion des systèmes d'information peuvent être soumis à de telles exigences.

Il convient de demander des conseils sur les exigences légales spécifiques auprès des conseillers juridiques de l'organisme ou des juristes qualifiés dans le domaine. Les exigences légales diffèrent d'un pays à l'autre et notamment en raison de la transmission d'informations entre les pays (flux de données transfrontières).

15.1.1 Identification de la législation en vigueur

Mesure

Pour chaque système d'information et pour l'organisme, il convient de définir, documenter et mettre à jour explicitement toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences.

Préconisations de mise en œuvre

De la même façon, il convient de définir et de documenter les mesures spécifiques et les responsabilités individuelles mises en place pour répondre à ces exigences.

15.1.2 Droits de propriété intellectuelle

Mesure

Il convient de mettre en œuvre des procédures appropriées visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel pouvant être soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires.

Préconisations de mise en œuvre

Il convient de prendre en compte les directives suivantes en vue de protéger tout matériel pouvant être soumis à des droits de propriété intellectuelle:

a) publier une politique de conformité des droits de propriété intellectuelle définissant l'utilisation légale des logiciels et logiciels d'information;

b) acquérir des logiciels uniquement à partir de sources connues et réputées afin de s'assurer du respect du droit de reproduction;

c) maintenir la sensibilisation à la politique appliquée en matière de protection des droits de propriété intellectuelle et annoncer la sanction à appliquer à l'encontre du personnel enfreignant cette politique;

d) tenir à jour des registres des biens appropriés et identifier tous les biens soumis à des exigences relatives aux droits de propriété intellectuelle;

e) conserver les preuves de la propriété des licences, des disques maître, des manuels, etc.;

f) mettre en œuvre des contrôles permettant de s'assurer que le nombre maximal d'utilisateurs habilités n'est pas dépassé;

g) effectuer des contrôles permettant de s'assurer que seuls des logiciels autorisés et sous licence sont installés;

h) mettre en œuvre une politique de gestion des conditions de licence appropriées;

i) mettre en œuvre une politique permettant de céder des logiciels ou de les transmettre à des tiers;

j) utiliser des outils d'audit appropriés;

k) se conformer aux conditions générales régissant les logiciels et les informations obtenus depuis des réseaux publics;

l) ne pas reproduire, convertir dans un autre format ou extraire des informations à partir d'enregistrements du commerce (film, enregistrement audio) si la loi sur le droit de reproduction ne l'autorise pas;

m) ne pas copier intégralement ou en partie des livres, articles, rapports ou autres documents si la loi sur le droit de reproduction ne l'autorise pas.

Informations supplémentaires

Les droits de propriété intellectuelle incluent le droit de reproduction régissant les logiciels et les documents, les droits de conception, les marques, les brevets et les licences régissant le code source.

Les logiciels propriétaires sont généralement dotés d'une licence d'utilisation stipulant les conditions générales de la licence telles que la limitation de l'utilisation des produits à des ordinateurs spécifiques ou la limitation de la reproduction à la seule création de copies de sauvegarde. Les droits de propriété intellectuelle relatifs aux logiciels développés par l'organisme doivent être clairement énoncés et expliqués au personnel.

Les exigences légales, réglementaires et contractuelles peuvent restreindre la copie du matériel propriétaire. Les exigences applicables peuvent notamment stipuler que seul le matériel développé par l'organisme ou le matériel pour lequel l'organisme dispose de licences fournies par le développeur peut être utilisé. La violation du droit de reproduction peut déclencher une action judiciaire pouvant aboutir à des poursuites pénales.

15.1.3 Protection des enregistrements de l'organisme

Mesure

Il convient de protéger les enregistrements importants de la perte, destruction et falsification conformément aux exigences légales, réglementaires et aux exigences métier.

Préconisations de mise en œuvre

Il convient de classer les enregistrements par types, tels que documents comptables, enregistrements de base de données, journaux de transactions, rapports d'audit et procédures d'exploitation; chaque type comporte des détails sur les périodes de conservation et le type de support de stockage: papier, microfiche, magnétique, optique. Il convient également de stocker tout matériel et programme liés aux clés de cryptographie et associés à des archives ou des signatures numériques chiffrées (voir 12.3) pour permettre le déchiffrement des enregistrements pendant la durée de conservation de ces enregistrements.

Il convient d'envisager l'éventualité d'une dégradation du support utilisé pour le stockage des enregistrements. Il convient de mettre en œuvre les procédures de stockage et de manipulation conformément aux recommandations du fabricant. Pour un stockage de longue durée, il convient d'utiliser le format papier et les microfiches.

Si des supports de stockage électroniques sont choisis, il convient d'inclure des procédures visant à garantir l'accès aux données (lisibilité du support et du format) tout au long de la période de conservation afin de protéger les données contre toute perte due à l'évolution de la technologie.

Il convient de choisir les systèmes de stockage des données de telle sorte qu'ils permettent la récupération des données requises dans un délai raisonnable et un format lisible conformément aux exigences à respecter.

Il convient que le système de stockage et de manipulation garantisse l'identification univoque des enregistrements et de leur durée de conservation tel que défini par la législation nationale ou régionale ou par les réglementations, le cas échéant. Il convient que ce système permette la destruction appropriée des enregistrements à l'issue de cette période s'ils ne sont plus utiles à l'organisme.

Pour remplir ces objectifs de sauvegarde des enregistrements, il convient que l'organisme suive les étapes suivantes:

a) il convient d'établir des directives relatives à la conservation, au stockage, à la manipulation et à l'élimination des enregistrements et informations;

b) il convient d'établir un calendrier de conservation identifiant les enregistrements et leur durée de conservation;

c) il convient de tenir à jour un inventaire des sources des informations clé;

d) il convient de prendre des mesures appropriées destinées à protéger les enregistrements et les informations contre la perte, la destruction et la falsification.

Informations supplémentaires

Certains enregistrements peuvent nécessiter une conservation sécurisée afin de satisfaire aux exigences légales, réglementaires ou contractuelles et de permettre les activités d'exploitation essentielles. Il peut s'agir d'enregistrements pouvant être requis dans le but de prouver qu'un organisme se conforme aux règles légales ou réglementaires, d'offrir une défense adéquate contre toute action civile ou pénale éventuelle ou de confirmer le statut financier d'un organisme auprès d'actionnaires, de tiers et de commissaires aux comptes. La période et le contenu des données pour la conservation des informations peuvent être définis par le droit ou la réglementation nationale.

Pour plus ample information concernant la gestion des enregistrements de l'organisme, voir l'ISO 15489-1.

15.1.4 Protection des données et confidentialité des informations relatives à la vie privée

Mesure

Il convient de garantir la protection et la confidentialité des données telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.

Préconisations de mise en œuvre

Il convient d'élaborer et de mettre en œuvre la protection des données de l'organisme et une politique de confidentialité. Il convient que cette politique soit connue de toutes les personnes impliquées dans le traitement des informations relatives à la vie privée.

La conformité avec cette politique et avec toutes les législations et réglementations relatives à la protection des données requiert un contrôle et une structure de gestion appropriés. La meilleure façon de mettre en place une telle structure est de désigner un responsable, par exemple un administrateur de la sécurité des données; il convient que cet administrateur conseille les responsables, utilisateurs et prestataires de services sur leurs responsabilités individuelles et les procédures spécifiques qu'il convient de respecter. Il convient que la responsabilité afférente à la gestion des informations relatives à la vie privée et au maintien de la sensibilisation aux principes de protection des données prenne en compte la législation et les réglementations applicables. Il convient de prendre les mesures techniques et organisationnelles appropriées pour protéger les informations relatives à la vie privée.

Informations supplémentaires

De nombreux pays ont introduit une législation imposant des contrôles sur la collecte, le traitement et la transmission des données relatives à la vie privée (il s'agit généralement d'informations permettant d'identifier les personnes). Selon la législation nationale concernée, ces contrôles peuvent inclure des taxes appliquées à ceux qui recueillent, traitent et diffusent des informations relatives à la vie privée; en outre, ces contrôles peuvent imposer des restrictions sur la transmission de données vers d'autres pays.

15.1.5 Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information

Mesure

Il convient de dissuader les utilisateurs de toute utilisation de moyens de traitement de l'information à des fins illégales.

Préconisations de mise en œuvre

Il convient que la direction approuve l'utilisation des moyens de traitement de l'information. Il convient de considérer comme inappropriée toute utilisation de ces équipements à des fins non professionnelles sans accord de la direction (voir 6.1.4) ou à des fins non autorisées. Si une activité non autorisée est identifiée par le biais de la surveillance ou par d'autres moyens, il convient d'en informer le responsable concerné en vue d'envisager l'action judiciaire et/ou la sanction appropriée.

Il convient de prendre les conseils d'un juriste avant de mettre en œuvre les procédures de surveillance.

Il convient également que tous les utilisateurs soient informés du domaine d'application exact de leur accès autorisé et de la surveillance mise en place en vue de détecter toute utilisation non autorisée. Les utilisateurs doivent être en possession d'une autorisation écrite. Il convient qu'une copie de ce document soit signée par l'utilisateur et conservée de façon sécurisée par l'organisme. Il convient d'informer les salariés d'un organisme, les contractants et les utilisateurs tiers qu'aucun accès autre que celui autorisé n'est toléré.

Lors de la connexion, il convient qu'un message d'avertissement s'affiche et indique que le moyen de traitement de l'information pour lequel un accès est demandé constitue la propriété de l'organisme et que, de ce fait, son accès est soumis à autorisation. L'utilisateur doit accuser réception du message et se conformer à celui-ci pour pouvoir poursuivre le processus de connexion (voir 11.5.1).

Informations supplémentaires

Les moyens de traitement de l'information d'un organisme sont prévus pour un usage essentiellement ou exclusivement professionnel.

La détection d'intrusion, l'analyse du contenu et d'autres outils de surveillance peuvent aider à empêcher et à détecter le mauvais usage des moyens de traitement de l'information.

De nombreux pays ont mise en place une législation destinée à empêcher un usage non conforme de l'ordinateur. L'utilisation d'un ordinateur à des fins non autorisées peut être considérée comme une infraction pénale.

La légalité de la surveillance de l'usage qu'il est fait des équipements varie d'un pays à l'autre. La direction peut être tenue d'avertir les utilisateurs de la surveillance mise en place et/ou d'obtenir leur accord. Dans le cas où le système pour lequel un accès est demandé est d'accès public (par exemple, un serveur web public) et est soumis à la surveillance liée à la sécurité, il convient qu'un message le signale.

15.1.6 Réglementation relative aux mesures cryptographiques

Mesure

Il convient de prendre des mesures cryptographiques conformément aux accords, lois et réglementations applicables.

Préconisations de mise en œuvre

En vue de se conformer aux accords, lois et réglementations applicables, il convient de prendre en compte les éléments suivants:

a) les restrictions en matière d'importation et/ou d'exportation de matériels et de logiciels destinés à l'exécution de fonctions cryptographiques;

b) les restrictions en matière d'importation et/ou d'exportation de matériels et de logiciels intégrant des fonctions cryptographiques;

c) les restrictions en matière d'utilisation du chiffrement;

d) les méthodes non discrétionnaires ou discrétionnaires dont disposent les autorités nationales pour accéder aux informations chiffrées par des moyens matériel ou logiciel dans le but de préserver la confidentialité du contenu.

Il convient de demander un avis juridique afin de s'assurer de la conformité avec les lois et réglementations nationales. Il convient également de bénéficier d'un avis juridique avant de transmettre des informations chiffrées ou des mesures cryptographiques dans un autre pays.

15.2 Conformité avec les politiques et normes de sécurité et conformité technique

Objectif: s'assurer de la conformité des systèmes avec les politiques et normes de sécurité de l'organisme.

Il convient de réexaminer régulièrement la sécurité des systèmes d'information.

Il convient d'effectuer ces réexamens en tenant compte des politiques de sécurité appliquées et de vérifier la conformité des plates-formes techniques et des systèmes d'information avec les normes de mise en œuvre de sécurité applicables et les mesures de sécurité documentées.

15.2.1 Conformité avec les politiques et les normes de sécurité

Mesure

Il convient que les responsables s'assurent de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité.

Préconisations de mise en œuvre

Il convient que les responsables réexaminent régulièrement la conformité du traitement de l'information dont ils sont chargés avec les politiques, normes de sécurité applicables et toute autre exigence de sécurité.

Si le réexamen détecte une non-conformité, il convient que les responsables

a) déterminent les causes de la non-conformité,

b) évaluent la nécessité d'engager des actions pour ne pas reproduire les causes de cette non-conformité,

c) déterminent et mettent en œuvre l'action corrective adéquate, et

d) réexaminent l'action corrective engagée.

Il convient que les résultats des réexamens et des actions correctives lancés par les responsables soient enregistrés et tenus à jour. Si le responsable supervise un réexamen indépendant, il convient qu'il communique les résultats de celui-ci à la personne ayant effectué ce réexamen (voir 6.1.8).

Informations supplémentaires

La surveillance de l'exploitation du système est abordée en 10.10.

15.2.2 Vérification de la conformité technique

Mesure

Il convient de vérifier régulièrement la conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité.

Préconisations de mise en œuvre

Il convient qu'un ingénieur système expérimenté lance la vérification de la conformité technique manuellement (à l'aide des outils logiciels appropriés, le cas échéant) et/ou à l'aide des outils automatisés générant un rapport technique en vue d'une interprétation ultérieure par un spécialiste.

Lors d'essais d'intrusion ou d'appréciations des vulnérabilités, il convient de procéder avec la plus grande prudence car de telles activités peuvent compromettre la sécurité du système. Il convient de planifier et de documenter ces essais qui doivent être répétables.

Il convient que toute vérification de la conformité technique soit effectuée par des personnes compétentes, habilitées ou de manière encadrée.

Informations supplémentaires

La vérification de la conformité technique implique l'examen des systèmes en exploitation en vue de garantir que les contrôles matériels et logiciels ont été correctement mis en œuvre. Ce type de vérification de la conformité requiert l'expertise d'un spécialiste.

La vérification de la conformité englobe les essais d'intrusion et les appréciations des vulnérabilités pouvant être effectués par des experts indépendants engagés à cette fin exclusivement. Ces essais peuvent aider à détecter les vulnérabilités du système et à vérifier l'efficacité des mesures prises pour empêcher les accès non autorisés dus à ces vulnérabilités.

Les essais d'intrusion et les appréciations des vulnérabilités fournissent un instantané du système dans un état précis et à une heure précise. L'instantané se limite aux portions du système effectivement soumises à essai lors du ou des essai(s) d'intrusion. Les essais d'intrusion et les appréciations des vulnérabilités ne remplacent en aucun cas l'appréciation du risque.

15.3 Prises en compte de l'audit du système d'information

Objectif: optimiser l'efficacité et réduire le plus possible l'interférence avec le/du processus d'audit du système d'information.

Il convient de prendre des mesures pour protéger les systèmes en exploitation et les outils d'audit lors des audits du système d'information.

De même, il est nécessaire de préserver l'intégrité et d'empêcher un mauvais usage des outils d'audit.

15.3.1 Contrôles de l'audit du système d'information

Mesure

Il convient que les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation soient planifiées de manière précise et qu'elles soient le résultat d'un accord afin de réduire le plus possible le risque de perturbations des processus métier.

Préconisations de mise en œuvre

Il convient de respecter les points suivants:

a) il convient que les exigences d'audit soient définies avec la direction concernée;

b) il convient de s'accorder sur le domaine d'application des contrôles et de le contrôler;

c) il convient que les contrôles soient limités à un accès en lecture seule du logiciel et des données;

d) il convient que tout accès, hormis en lecture seule, soit autorisé uniquement pour les copies isolées des fichiers système qui seront supprimées une fois l'audit terminé ou qu'une protection appropriée de ces fichiers soit apportée si la documentation de l'audit exige leur conservation;

e) il convient d'identifier explicitement et de mettre à disposition les ressources destinées à l'exécution de ces contrôles;

f) il convient d'identifier et de s'accorder sur les exigences liées à un traitement spécial ou supplémentaire;

g) il convient de surveiller et de journaliser tous les accès afin de disposer d'une trace de référence; il convient de prendre en compte les traces de référence horodatées pour les données ou systèmes critiques;

h) il convient de documenter toutes les procédures, exigences et responsabilités;

i) il convient que la ou les personne(s) chargée(s) de l'audit ne soient pas impliquée(s) dans les activités vérifiées.

15.3.2 Protection des outils d'audit du système d'information

Mesure

Il convient de protéger l'accès aux outils d'audit du système d'information afin d'empêcher tous mauvais usage ou compromission éventuels.

Préconisations de mise en œuvre

Il convient que les outils d'audit du système d'information tels que les logiciels ou les fichiers de données soient séparés du système de développement et du système en exploitation et ne soient pas conservés dans la bandothèque ou les zones utilisateurs, à moins que ces outils soient dotés d'un niveau approprié de protection supplémentaire.

Informations supplémentaires

Si un tiers est impliqué dans un audit, il existe un risque de mauvais usage par ce tiers des outils d'audit et des informations auxquelles cet organisme tiers accède. Il convient de prendre des mesures comme en 6.2.1 (pour apprécier les risques) et en 9.1.2 (pour limiter l'accès physique) pour éviter ce risque et toute conséquence telle que le changement immédiat des mots de passe divulgués aux commissaires aux comptes.

Bibliographie

[1] ISO/CEI Guide 2:2004, *Normalisation et activités connexes — Vocabulaire général*

[2] ISO/CEI Guide 73:2002, *Management du risque — Vocabulaire — Principes directeurs pour l'utilisation dans les normes*

[3] ISO/CEI 9796-2:2002, *Technologies de l'information — Techniques de sécurité — Schémas de signature numérique rétablissant le message — Partie 2: Mécanismes basés sur une factorisation entière*

[4] ISO/CEI 9796-3:2000, *Technologies de l'information — Techniques de sécurité — Schémas de signature numérique rétablissant le message — Partie 3: Mécanismes basés sur les logarithmes discrets*

[5] ISO 10007:2003, *Systèmes de management de la qualité — Lignes directrices pour la gestion de la configuration*

[6] ISO/CEI 11770-1:1996, *Technologies de l'information — Techniques de sécurité — Partie 1: Cadre général*

[7] ISO/CEI 12207:1995, *Technologies de l'information — Processus du cycle de vie du logiciel*

[8] ISO/CEI 13335-1:2004, *Technologies de l'information — Techniques de sécurité — Gestion de la sécurité des technologies de l'information et des communications — Partie 1: Concepts et modèles pour la gestion de la sécurité des technologies de l'information et des communications*

[9] ISO/CEI TR 13335-3:1998, *Technologies de l'information — Lignes directrices pour la gestion de sécurité IT — Partie 3: Techniques pour la gestion de sécurité IT*

[10] ISO/CEI 13888-1:1997, *Technologies de l'information — Techniques de sécurité — Non-répudiation — Partie 1: Généralités*

[11] ISO/CEI TR 14516:2002, *Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'utilisation et la gestion des services de tiers de confiance*

[12] ISO/CEI 14888-1:1998, *Technologies de l'information — Techniques de sécurité — Signatures digitales avec appendice — Partie 1: Généralités*

[13] ISO/CEI 15408-1:1999, *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 1: Introduction et modèle général*

[14] ISO 15489-1:2001, *Information et documentation — «Records management» — Partie 1: Principes directeurs*

[15] ISO/CEI 18028-4, *Technologies de l'information — Techniques de sécurité — Sécurité de réseaux TI — Partie 4: Téléaccès de la sécurité*

[16] ISO/CEI TR 18044, *Technologies de l'information — Techniques de sécurité — Gestion d'incidents de sécurité de l'information*

[17] ISO 19011:2002, *Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental*

[18] IEEE P1363-2000, *Standard Specifications for Public-Key Cryptography*

[19] Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information: «*Vers une culture de la sécurité*», 2002

[20] Lignes directrices de l'OCDE régissant la politique de cryptographie, 1997