NORME INTERNATIONALE

ISO/CEI 27002

Deuxième édition
2013-10-01

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

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

Numéro de référence
ISO/CEI 27002:2013(F)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Publié en Suisse

Sommaire

Page

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 ne saurait être tenue pour responsable 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 ISO/CEI 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 27002:2005), qui a fait l'objet d'une révision technique et structurelle.

0 Introduction

0.1 Historique et contexte

La présente Norme internationale a pour objet de servir d'outil de référence permettant aux organisations de sélectionner les mesures nécessaires dans le cadre d'un processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon l'ISO/CEI 27001[10] ou de guide pour les organisations mettant en œuvre des mesures de sécurité de l'information largement reconnues. La présente norme a également pour objet d'élaborer des lignes directrices de management de la sécurité de l'information spécifiques aux organisations et aux entreprises, en tenant compte de leur(s) environnement(s) particulier(s) de risques de sécurité de l'information.

Des organisations de tous types et de toutes dimensions (incluant le secteur public et le secteur privé, à but lucratif ou non lucratif) collectent, traitent, stockent et transmettent l'information sous de nombreuses formes, notamment électronique, physique et verbale (par exemple, au cours de conversations et de présentations).

La valeur de l'information dépasse les mots, les chiffres et les images: la connaissance, les concepts, les idées et les marques sont des exemples de formes d'information immatérielles. Dans un monde interconnecté, l'information et les processus, systèmes et réseaux qui s'y rattachent, ainsi que le personnel impliqué dans son traitement, ses manipulations et sa protection, sont des actifs précieux pour l'activité d'une organisation, au même titre que d'autres actifs d'entreprise importants, et, par conséquent, ils méritent ou nécessitent d'être protégés contre les divers risques encourus.

Les actifs sont exposés à des menaces tant accidentelles que délibérées, alors que les processus, les systèmes, les réseaux et les personnes qui s'y rattachent présentent des vulnérabilités qui leur sont propres. Des changements apportés aux processus et aux systèmes de l'organisation ou d'autres changements externes (comme l'application de nouvelles lois et réglementations) peuvent engendrer de nouveaux risques pour la sécurité de l'information. Par conséquent, étant donné que les menaces disposent d'une multitude de possibilités d'exploitation des vulnérabilités pour nuire à l'organisation, les risques de sécurité de l'information sont omniprésents. Une sécurité efficace de l'information réduit ces risques en protégeant l'organisation contre les menaces et les vulnérabilités, ce qui réduit les conséquences sur ses actifs.

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'une organisation. Un système de management de la sécurité de l'information (SMSI) tel que celui spécifié dans l'ISO/CEI 27001[10] appréhende les risques de sécurité de l'information de l'organisation dans une vision globale et coordonnée, de manière à mettre en œuvre un ensemble complet de mesures liées à la sécurité de l'information dans le cadre général d'un système de management cohérent.

Nombreux sont les systèmes d'information qui n'ont pas été conçus dans un souci de sécurité au sens de l'ISO/CEI 27001[10] et de la présente norme. La sécurité qui peut être mise en œuvre par des moyens techniques est limitée et il convient de la soutenir à l'aide de moyens de management et de procédures adaptés. L'identification des mesures qu'il convient de mettre en place nécessite de procéder à une planification minutieuse et de prêter attention aux détails. Un système de management de la sécurité de l'information efficace requiert l'adhésion de tous les salariés de l'organisation. Il peut également nécessiter la participation des actionnaires, des fournisseurs ou d'autres tiers. De même, l'avis de spécialistes tiers peut se révéler nécessaire.

De manière plus générale, une sécurité de l'information efficace garantit également à la direction et aux parties tiers que les actifs de l'organisation sont, dans des limites raisonnables, sécurisés et à l'abri des préjudices, et contribuent de ce fait au succès de l'organisation.

0.2 Exigences liées à la sécurité de l'information

Une organisation doit impérativement identifier ses exigences en matière de sécurité. Ces exigences proviennent de trois sources principales:

a) l'appréciation du risque propre à l'organisation, prenant en compte sa stratégie et ses objectifs généraux. L'appréciation du risque permet d'identifier les menaces pesant sur les actifs, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel;

b) les exigences légales, statutaires, réglementaires et contractuelles auxquelles l'organisation et ses partenaires commerciaux, contractants et prestataires de service, doivent répondre ainsi que leur environnement socioculturel;

c) l'ensemble de principes, d'objectifs et d'exigences métier en matière de manipulation, de traitement, de stockage, de communication et d'archivage de l'information que l'organisation s'est constitué pour mener à bien ses activités.

Il est nécessaire de confronter les ressources mobilisées par la mise en œuvre des mesures avec les dommages susceptibles de résulter de défaillances de la sécurité en l'absence de ces mesures. Les résultats d'une appréciation du risque permettent de définir les actions de gestion appropriées et les priorités en matière de gestion des risques liés à la sécurité de l'information, ainsi que de mettre en œuvre les mesures identifiées destinées à contrer ces risques.

La norme ISO/CEI 27005[11] fournit des lignes directrices de gestion du risque lié à la sécurité de l'information, y compris des conseils sur l'appréciation du risque, le traitement du risque, l'acceptation du risque, la communication relative au risque, la surveillance du risque et la revue du risque.

0.3 Sélection des mesures

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 dépend des décisions prises par l'organisation en fonction de ses critères d'acceptation du risque, de ses options de traitement du risque et de son approche de la gestion générale du risque. Il convient également de prendre en considération les lois et règlements nationaux et internationaux concernés. La sélection des mesures de sécurité dépend également de la manière dont les mesures interagissent pour assurer une défense en profondeur.

Certaines mesures décrites dans la présente norme peuvent être considérées comme des principes directeurs pour le management de la sécurité de l'information et être appliquées à la plupart des organisations. Les mesures et des lignes directrices de mise en œuvre sont détaillées ci-dessous. De plus amples informations sur la sélection des mesures et d'autres options de traitement du risque figurent dans l'ISO/CEI 27005.[11]

0.4 Mise au point de lignes directrices propres à l'organisation

La présente Norme internationale peut servir de base pour la mise au point de lignes directrices spécifiques à une organisation. Une partie des mesures et lignes directrices de ce code de bonnes pratiques peut ne pas être applicable. 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 peut 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.

0.5 Examen du cycle de vie

L'information est soumise à un cycle de vie naturel, depuis sa création et son origine en passant par son stockage, son traitement, son utilisation, sa transmission, jusqu'à sa destruction finale ou son obsolescence. La valeur des actifs et les risques qui y sont liés peuvent varier au cours de la durée de vie de ces actifs (par exemple, une divulgation non autorisée ou le vol des comptes financiers d'une entreprise revêt une importance bien moins grande après leur publication officielle), mais dans une certaine mesure l'importance de la sécurité de l'information subsiste à tous les stades.

Les systèmes d'information sont soumis à des cycles de vie durant lesquels ils sont pensés, caractérisés, conçus, mis au point, testés, mis en œuvre, utilisés, entretenus et finalement retirés du service et mis au rebut. Il convient que la sécurité de l'information soit prise en compte à tous les stades. La mise au point de nouveaux systèmes et les changements apportés aux systèmes existants donnent l'occasion aux organisations de mettre à jour les mesures de sécurité et de les améliorer en tenant compte des incidents réels survenus et des risques de sécurité de l'information actuels et anticipés.

0.6 Normes associées

Alors que la présente Norme internationale propose des lignes directrices portant sur un vaste éventail de mesures de sécurité liées à l'information d'utilisation courante dans nombre d'organisations différentes, les autres normes de la famille ISO/CEI 27000 présentent des conseils complémentaires ou des exigences relatifs à d'autres aspects de l'ensemble du processus de management de la sécurité de l'information.

Se reporter à l'ISO/CEI 27000 pour une introduction générale aux systèmes de management de la sécurité de l'information et à la famille de normes. L'ISO/CEI 27000 présente un glossaire, définissant de manière formelle la plupart des termes utilisés dans la famille de normes ISO/CEI 27000, et décrit le domaine d'application et les objectifs de chaque élément de cette famille.

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

1 Domaine d'application

La présente Norme internationale donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation.

La présente Norme internationale est élaborée à l'intention des organisations désireuses

a) de sélectionner les mesures nécessaires dans le cadre du processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon l'ISO/CEI 27001;[10]

b) de mettre en œuvre des mesures de sécurité de l'information largement reconnues;

c) d'élaborer leurs propres lignes directrices de management de la sécurité de l'information.

2 Références normatives

Les documents suivants, en tout ou partie, sont référencés de manière normative dans le présent document et sont indispensables à son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/CEI 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/CEI 27000 s'appliquent.

4 Structure de la présente norme

La présente norme contient 14 articles relatifs aux mesures de sécurité, comprenant un total de 35 catégories de sécurité principales et 114 mesures.

4.1 Articles

Chaque article définissant des mesures de sécurité contient une ou plusieurs catégories de sécurité principales.

L'ordre des articles dans la présente norme n'est aucunement lié à leur importance. Selon les circonstances, les mesures de sécurité, qu'elles figurent dans un article quel qu'il soit ou dans tous les articles, peuvent s'avérer importantes: par conséquent, il convient que chaque organisation appliquant la présente norme identifie les mesures appropriées, leur importance et leur application aux processus métier ciblés. Plus généralement, les listes contenues dans la présente norme ne sont pas classées par ordre de priorité.

4.2 Catégories de mesures

Chaque catégorie principale de mesures comprend:

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

b) une ou plusieurs mesures pouvant être appliquées 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. Les préconisations peuvent ne pas être tout à fait adaptées ou suffisantes dans toutes les situations et peuvent ne pas répondre aux exigences spécifiques de l'organisation en matière de sécurité.

Informations supplémentaires

Présente des compléments d'information à considérer, par exemple des éléments juridiques et des références à d'autres normes. En l'absence de compléments d'information, cette rubrique n'apparaît pas.

5 Politiques de sécurité de l'information

5.1 Orientations de la direction en matière 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.

5.1.1 Politiques de sécurité de l'information

Mesure

Il convient de définir un ensemble de politiques en matière de sécurité de l'information qui soit approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.

Préconisations de mise en œuvre

Il convient que les organisations définissent, à leur plus haut niveau, une «politique de sécurité de l'information», qui soit approuvée par la direction et qui décrive l'approche adoptée pour gérer les objectifs de sécurité de l'information.

Il convient que les politiques de sécurité de l'information traitent des exigences créées par:

a) la stratégie d'entreprise;

b) les réglementations, la législation et les contrats;

c) l'environnement réel et anticipé des menaces liées à la sécurité de l'information.

Il convient que cette politique de sécurité de l'information comporte des précisions concernant:

a) une définition de la sécurité de l'information, ses objectifs et ses principes pour orienter toutes les activités relatives à la sécurité de l'information;

b) l'attribution de responsabilités générales et spécifiques en matière de management de la sécurité de l'information à des fonctions définies;

c) des processus de traitement des dérogations et des exceptions.

Il convient qu'à un niveau inférieur, la politique de sécurité de l'information soit étayée par des politiques portant sur des thèmes spécifiques, qui imposent en outre la mise en œuvre de mesures de sécurité de l'information et sont de manière générale structurées pour répondre aux besoins de certains groupes cibles d'une organisation ou pour englober certains thèmes.

Voici des exemples de politiques à thèmes:

a) le contrôle d'accès (voir l'Article 9);

b) la classification (et le traitement) de l'information (voir 8.2);

c) la sécurité physique et environnementale (voir l'Article 11);

d) thèmes axés sur l'utilisateur final:

   1) utilisation correcte des actifs (voir 8.1.3);

   2) bureau propre et écran vide (voir 11.2.9);

   3) transfert de l'information (voir 13.2.1);

   4) appareils mobiles et télétravail (voir 6.2);

   5) restrictions en matière d'installation et d'utilisation de logiciels (voir 12.6.2);

e) sauvegarde (voir 12.3);

f) transfert de l'information (voir 13.2);

g) protection contre les logiciels malveillants (voir 12.2);

h) gestion des vulnérabilités techniques (voir 12.6.1);

i) mesures de sécurité cryptographiques (voir l'Article 10);

j) sécurité des communications (voir l'Article 13);

k) protection de la vie privée et des informations personnelles identifiables (voir 18.1.4);

l) relations avec les fournisseurs (voir l'Article 15).

Il convient que ces politiques soient communiquées aux salariés et aux tiers concernés sous une forme pertinente, accessible et compréhensible par leurs destinataires, par exemple dans le contexte d'un «programme d'apprentissage, de formation et de sensibilisation à la sécurité de l'information» (voir 7.2.2).

Informations supplémentaires

Le besoin en politiques internes liées à la sécurité de l'information varie en fonction des organisations. Les politiques internes sont particulièrement utiles pour les organisations les plus grandes et les plus complexes, dans lesquelles les personnes qui définissent et approuvent les niveaux attendus des mesures sont isolées des personnes mettant en œuvre ces mesures, ou dans les situations où une politique s'applique à un certain nombre de personnes ou de fonctions différentes dans l'organisation. Les politiques de sécurité de l'information peuvent être diffusées dans un document unique «politique de sécurité de l'information» ou dans un ensemble de documents séparés, mais interdépendants.

Si l'une quelconque des politiques de sécurité de l'information est diffusée hors de l'organisation, il convient de veiller à ne pas divulguer d'informations confidentielles.

Certaines organisations utilisent des termes différents pour désigner ces documents de politiques, tels que «normes», «directives» ou «règles».

5.1.2 Revue des politiques de sécurité de l'information

Mesure

Pour garantir la constance de la pertinence, de l'adéquation et de l'efficacité des politiques liées à la sécurité de l'information, il convient de revoir ces politiques à intervalles programmés ou en cas de changements majeurs.

Préconisations de mise en œuvre

Il convient que chaque politique ait un propriétaire ayant accepté la responsabilité de développer, revoir et évaluer cette politique. Il convient que la revue comporte une appréciation des possibilités d'amélioration de la politique de l'organisation et une approche de management de la sécurité de l'information pour répondre aux changements intervenant dans l'environnement organisationnel, aux circonstances liées à l'activité, au contexte juridique ou à l'environnement technique.

Il convient que la revue des politiques de sécurité de l'information tienne compte des revues de direction.

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: Établir un cadre de gestion pour engager, puis vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation.

6.1.1 Fonctions et responsabilités liées à la sécurité de l'information

Mesure

Il convient de définir et d'attribuer 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 5.1.1). Il convient de déterminer les responsabilités en ce qui concerne la protection des actifs individuels et la mise en œuvre de processus de sécurité spécifiques. Il convient de déterminer les responsabilités liées aux activités de gestion des risques en matière de sécurité de l'information et, en particulier, celles liées à l'acceptation des risques résiduels. Si nécessaire, il convient de compléter ces responsabilités de directives détaillées, appropriées à certains sites et moyens de traitement de l'information. Il convient de déterminer les responsabilités locales en ce qui concerne la protection des actifs et la mise en œuvre des processus de sécurité spécifiques.

Les personnes auxquelles ont été attribuées des responsabilités en matière de sécurité peuvent déléguer des tâches de sécurité. Néanmoins, elles demeurent responsables et il convient qu'elles s'assurent de la bonne exécution de toute tâche déléguée.

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

a) il convient d'identifier et de déterminer les actifs et les processus de sécurité;

b) il convient d'affecter une entité responsable à chaque actif ou processus et de documenter ses responsabilités dans le détail (voir 8.1.2);

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

d) Pour être à même d'assurer les responsabilités relevant de leur domaine en matière de sécurité, il convient que les personnes désignées soient compétentes dans ce domaine et qu'elles bénéficient de possibilités leur permettant de se tenir au courant des évolutions;

e) Il convient d'identifier et de documenter les activités de coordination et de supervision relatives aux questions de sécurité liées aux relations avec les fournisseurs.

Informations supplémentaires

De nombreuses organisations désignent un responsable de la sécurité de l'information pour assumer la responsabilité d'ensemble de l'élaboration et de la mise en œuvre de la politique de sécurité de l'information et pour corroborer l'identification des mesures de sécurité.

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

6.1.2 Séparation des tâches

Mesure

Il convient de séparer les tâches et les domaines de responsabilité incompatibles pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.

Préconisations de mise en œuvre

Il convient de veiller à ce que personne ne puisse accéder à, modifier ou utiliser des actifs sans en avoir reçu l'autorisation ou sans avoir été détecté. Il convient de séparer le déclenchement d'un événement de son autorisation. Il convient d'envisager la possibilité de collusion lors de la conception des mesures.

Les organisations de petite taille peuvent avoir des difficultés à réaliser une séparation des 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, des systèmes de traçabilité et la supervision de la direction.

Informations supplémentaires

La séparation des tâches est une méthode permettant de diminuer les risques de mauvais usage, accidentel ou délibéré, des actifs d'une organisation.

6.1.3 Relations avec les autorités

Mesure

Il convient d'entretenir des relations appropriées avec les autorités compétentes.

Préconisations de mise en œuvre

Il convient que les organisations mettent en place des procédures spécifiant quand et comment il convient de contacter les autorités compétentes (par exemple, les autorités chargées de l'application des lois, les organismes de réglementation, les autorités de surveillance). Ces procédures définissent également comment il convient de signaler dans les meilleurs délais les incidents liés à la sécurité de l'information (par exemple, en cas de suspicion de violation de la loi).

Informations supplémentaires

Les organisations subissant une attaque par le biais d'Internet peuvent recourir aux autorités pour engager des actions à l'encontre de la source de l'attaque.

Entretenir de telles relations peut constituer une exigence afin de favoriser la gestion des incidents (voir l'Article 16) ou le processus de planification des mesures d'urgence et de continuité de l'activité

(voir l'Article 17). Les relations avec les autorités de régulation sont également utiles pour anticiper et préparer les changements à venir sur le plan juridique ou réglementaire, qui doivent être mis en œuvre par l'organisation. Les relations avec les autres autorités concernent les services collectifs, les services d'urgence, les fournisseurs d'électricité, la santé et la sécurité, comme la caserne de 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).

6.1.4 Relations avec des groupes de travail spécialisés

Mesure

Il convient d'entretenir des relations appropriées avec des groupes d'intérêt, 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 à des forums spécialisés aux fins suivantes:

a) mieux connaître les bonnes pratiques et se tenir informé de l'évolution des savoirs relatifs 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 rapidement des alertes, des conseils et des correctifs logiciels portant sur 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 16).

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 confidentielles.

6.1.5 La sécurité de l'information dans la gestion de projet

Mesure

Il convient de traiter la sécurité de l'information dans la gestion de projet, quel que soit le type de projet concerné.

Préconisations de mise en œuvre

Il convient d'intégrer la sécurité de l'information dans la ou les méthodes de gestion de projet de l'organisation pour veiller à ce que les risques de sécurité de l'information soient identifiés et traités dans le cadre du projet. Cette préconisation s'applique de manière générale à tout projet quel qu'il soit, indépendamment de sa nature, par exemple un projet lié à un processus clé de l'activité, aux technologies de l'information, à la gestion des installations et autres processus. Il convient que les méthodes de gestion de projet en vigueur imposent que:

a) les objectifs en matière de sécurité de l'information soient intégrés aux objectifs du projet;

b) une appréciation du risque de sécurité de l'information soit effectuée au commencement du projet pour identifier les mesures nécessaires;

c) la sécurité de l'information soit intégrée à toutes les phases de la méthodologie de projet appliquée.

Pour tous les projets, il convient de traiter et de revoir régulièrement les incidences sur la sécurité de l'information. Il convient de déterminer et d'attribuer les responsabilités en matière de sécurité de l'information à des fonctions spécifiques définies dans les méthodes de gestion de projet.

6.2 Appareils mobiles et télétravail

Objectif: Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles.

6.2.1 Politique en matière d'appareils mobiles

Mesure

Il convient d'adopter une politique et des mesures de sécurité complémentaires pour gérer les risques découlant de l'utilisation des appareils mobiles.

Préconisations de mise en œuvre

Lors de l'utilisation d'appareils mobiles, il convient de veiller particulièrement à ce que les informations liées à l'activité de l'organisation ne soient pas compromises. Il convient que la politique en matière d'appareils mobiles tienne compte des risques liés au fait de travailler avec des appareils mobiles dans des environnements non protégés.

Il convient que la politique en matière d'appareils mobiles envisage:

a) l'enregistrement des appareils mobiles;

b) les exigences liées à la protection physique;

c) les restrictions liées à l'installation de logiciels;

d) les exigences liées aux versions logicielles des appareils mobiles et à l'application de correctifs;

e) les restrictions liées aux connexions à des services d'information;

f) les contrôles d'accès;

g) les techniques cryptographiques;

h) la protection contre les logiciels malveillants;

i) la désactivation, l'effacement des données ou le verrouillage à distance;

j) les sauvegardes;

k) l'utilisation des services web et des applications web.

Il convient d'être vigilant lors de l'utilisation d'appareils mobiles dans des lieux publics, des salles de réunions et autres zones non protégées. Il convient de mettre en place des mesures de protection visant à empêcher les accès non autorisés ou la divulgation d'informations stockées et traitées par ces appareils, par exemple en utilisant des techniques cryptographiques (voir l'Article 10) et en imposant l'utilisation d'informations d'authentification secrètes (voir 9.2.3).

Il convient également que les appareils mobiles soient physiquement protégés contre le vol, en particulier lorsqu'ils sont laissés, par exemple, 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 spécifique tenant compte des exigences juridiques, des exigences liées aux assurances et des exigences de sécurité de l'organisation, en cas de vol ou de perte d'appareils mobiles. Il convient de ne pas laisser sans surveillance les appareils dans lesquels sont stockées des informations importantes, sensibles ou critiques liées à l'activité de l'organisation et, si possible, de les mettre sous clé ou de les doter de systèmes de verrouillage spéciaux.