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 ..... **v**

0 Introduction ..... **vi**

1 Domaine d'application **1**

2 Références normatives **1**

3 Termes et définitions **1**

4 Structure de la présente norme **1**
4.1 Articles 1
4.2 Catégories de mesures 2

5 Politiques de sécurité de l'information **2**
5.1 Orientations de la direction en matière de sécurité de l'information 2

6 Organisation de la sécurité de l'information **4**
6.1 Organisation interne 4
6.2 Appareils mobiles et télétravail 7

7 La sécurité des ressources humaines **9**
7.1 Avant l'embauche 9
7.2 Pendant la durée du contrat 11
7.3 Rupture, terme ou modification du contrat de travail 14

8 Gestion des actifs **15**
8.1 Responsabilités relatives aux actifs 15
8.2 Classification de l'information 16
8.3 Manipulation des supports 19

9 Contrôle d'accès **21**
9.1 Exigences métier en matière de contrôle d'accès 21
9.2 Gestion de l'accès utilisateur 23
9.3 Responsabilités des utilisateurs 27
9.4 Contrôle de l'accès au système et aux applications 28

10 Cryptographie **31**
10.1 Mesures cryptographiques 31

11 Sécurité physique et environnementale **34**
11.1 Zones sécurisées 34
11.2 Matériels 37

12 Sécurité liée à l'exploitation **42**
12.1 Procédures et responsabilités liées à l'exploitation 42
12.2 Protection contre les logiciels malveillants 46
12.3 Sauvegarde 47
12.4 Journalisation et surveillance 48
12.5 Maîtrise des logiciels en exploitation 50
12.6 Gestion des vulnérabilités techniques 51
12.7 Considérations sur l'audit du système d'information 53

13 Sécurité des communications **54**
13.1 Management de la sécurité des réseaux 54
13.2 Transfert de l'information 56

14 Acquisition, développement et maintenance des systèmes d'information **60**
14.1 Exigences de sécurité applicables aux systèmes d'information 60
14.2 Sécurité des processus de développement et d'assistance technique 63
14.3 Données de test 68

15 Relations avec les fournisseurs **69**
15.1 Sécurité de l'information dans les relations avec les fournisseurs 69

15.2 Gestion de la prestation du service ... 72
16 Gestion des incidents liés à la sécurité de l'information ... 74
16.1 Gestion des incidents liés à la sécurité de l'information et améliorations ... 74
17 Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité ... 78
17.1 Continuité de la sécurité de l'information ... 78
17.2 Redondances ... 80
18 Conformité ... 81
18.1 Conformité aux obligations légales et réglementaires ... 81
18.2 Revue de la sécurité de l'information ... 84
Bibliographie ... 87

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.

