NORME INTERNATIONALE

ISO/CEI 27002

Première édition
2005-06-15

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

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

Numéro de référence
ISO/CEI 27002:2005(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

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

NORME INTERNATIONALE

ISO/CEI 17799

Deuxième édition
2005-06-15

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

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

Numéro de référence
ISO/CEI 17799:2005(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) 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.