NORME INTERNATIONALE

ISO/IEC 27002

Troisième édition
2022-02

Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information

Information security, cybersecurity and privacy protection — Information security controls

Numéro de référence
ISO/IEC 27002:2022(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +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 l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC 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 l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'attention est attirée 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 l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets) ou dans la liste des déclarations de brevets reçues par l'IEC (voir https://patents.iec.ch).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27002:2013), qui a fait l'objet d'une révision technique. Elle incorpore également les Rectificatifs techniques ISO/IEC 27002:2013/Cor. 1:2014 et ISO/IEC 27002:2013/Cor. 2:2015.

Les principales modifications sont les suivantes:

— le titre a été modifié;

— la structure du document a été modifiée, présentant les mesures de sécurité avec une taxonomie simple et des attributs associés;

— certaines mesures de sécurité ont été fusionnées, d'autres ont été supprimées, et plusieurs nouvelles mesures de sécurité ont été ajoutées. La correspondance complète se trouve à l'Annexe B.

La présente version française de l'ISO/IEC 27002:2022 correspond à la version anglaise publiée le 2022-02 et corrigé le 2022-03.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/members.html et www.iec.ch/national-committees.

Introduction

0.1 Historique et contexte

Le présent document a été conçu à l'intention des organisations de tous types et de toutes dimensions. Il est à utiliser comme document de référence pour déterminer et mettre en œuvre des mesures de sécurité pour le traitement des risques de sécurité de l'information dans un système de management de la sécurité de l'information (SMSI) basé sur l'ISO/IEC 27001. Il peut également être utilisé comme guide de bonnes pratiques pour les organisations qui déterminent et mettent en œuvre les mesures de sécurité de l'information communément admises. De plus, le présent document a pour objet d'être utilisé lors de l'élaboration des lignes directrices de gestion de la sécurité de l'information spécifiques aux organisations et aux industries, en tenant compte de leur(s) environnement(s) spécifique(s) de risques de sécurité de l'information. Des mesures de sécurité organisationnelles ou spécifiques à l'environnement autres que celles qui figurent dans le présent document peuvent, si nécessaire, être déterminées par le biais de l'appréciation du risque.

Des organisations de tous types et de toutes dimensions (y compris du secteur public et du secteur privé, à but lucratif ou non lucratif) créent, collectent, traitent, stockent, transmettent et éliminent l'information sous de nombreuses formes, notamment électronique, physique et verbale (par exemple, les conversations et les présentations).

La valeur de l'information va au-delà des mots, chiffres et images écrits: la connaissance, les concepts, les idées et les marques sont des exemples de formes intangibles d'information. Dans un monde interconnecté, les informations et autres actifs associés méritent ou exigent une protection contre différentes sources de risques, aussi bien naturelles, qu'accidentelles ou délibérées.

La sécurité de l'information est réalisée par la mise en œuvre d'un ensemble de mesures de sécurité appropriées, notamment des politiques, des règles, des processus, des procédures, des structures organisationnelles, et des fonctions matérielles et logicielles. Pour atteindre ses objectifs métier et de sécurité, il convient que l'organisation définisse, mette en œuvre, surveille, révise et améliore ces mesures de sécurité au besoin. Un système de management de la sécurité de l'information (SMSI) tel que celui spécifié dans l'ISO/IEC 27001 appréhende les risques de sécurité de l'information de l'organisation dans une vision globale et coordonnée, afin de déterminer et mettre en œuvre un ensemble complet de mesures de sécurité de l'information dans le cadre global d'un système de management cohérent.

De nombreux systèmes d'information, y compris leur management et leurs opérations, n'ont pas été conçus sécurisés au sens d'un système de management de la sécurité de l'information tel que spécifié dans l'ISO/IEC 27001 et le présent document. Le niveau de sécurité qui peut être atteint seulement par des mesures techniques est limité, et il convient de le renforcer par des processus organisationnels et des activités de management appropriés. L'identification des mesures de sécurité qu'il convient de mettre en place nécessite une planification minutieuse et une attention aux détails lors de la réalisation du traitement du risque.

Un système de management de la sécurité de l'information réussi requiert l'adhésion de tout le personnel de l'organisation. Il peut également nécessiter la participation d'autres parties intéressées, telles que des actionnaires ou des fournisseurs. Des conseils d'experts en la matière peuvent aussi s'avérer nécessaires.

Un système de management de la sécurité de l'information approprié, adéquat et efficace procure la garantie aux dirigeants de l'organisation et autres parties intéressées que leurs informations et autres actifs associés sont suffisamment sécurisés et protégés contre les menaces et dommages, ce qui permet à l'organisation d'atteindre les objectifs métier visés.

0.2 Exigences de sécurité de l'information

Il est essentiel qu'une organisation détermine ses exigences de sécurité de l'information. Il existe trois principales sources des exigences de sécurité de l'information:

a) l'appréciation du risque de l'organisation, prenant en compte l'ensemble de sa stratégie et objectifs métier. Cela peut être facilité ou appuyé par une appréciation du risque de sécurité de l'information.