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)

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.

Il convient que cela aboutisse à la détermination des mesures de sécurité nécessaires assurant que les risques résiduels pour l'organisation correspondent à ses critères d'acceptation des risques;

b) les exigences légales, statutaires, réglementaires et contractuelles auxquelles l'organisation et ses parties intéressées (partenaires commerciaux, fournisseurs de services, etc.) doivent se conformer ainsi que leur environnement socioculturel;

c) l'ensemble des principes, d'objectifs et d'exigences métier pour toutes les étapes du cycle de vie de l'information que l'organisation a élaboré pour appuyer son fonctionnement.

0.3 Mesures de sécurité

Un mesure de sécurité est définie comme une mesure qui modifie ou maintient un risque. Certaines des mesures de sécurité dans le présent document sont des moyens qui modifient les risques, tandis que d'autres maintiennent les risques. Une politique de sécurité de l'information, par exemple, permet seulement de maintenir les risques, tandis que la conformité à la politique de sécurité de l'information peut modifier les risques. De plus, certaines mesures de sécurité décrivent la même mesure générique dans différents contextes de risques. Le présent document propose une combinaison générique de mesures de sécurité de l'information organisationnelles, liées aux personnes, physiques et technologiques, issues des bonnes pratiques reconnues au niveau international.

0.4 Détermination des mesures de sécurité

La détermination des mesures de sécurité dépend des décisions de l'organisation suite à une appréciation du risque, avec un périmètre clairement défini. Il convient de baser les décisions relatives aux risques identifiés sur les critères d'acceptation des risques, les options de traitement des risques et l'approche de gestion des risques appliqués par l'organisation. Il convient également que la détermination des mesures de sécurité tienne compte de toutes les législations et réglementations nationales et internationales pertinentes. La détermination des mesures de sécurité dépend aussi de la manière dont les mesures de sécurité interagissent les unes avec les autres pour assurer une défense en profondeur.

L'organisation peut concevoir des mesures de sécurité au besoin, ou bien les identifier à partir de n'importe quelle source. Lors de la spécification de ces mesures de sécurité, il convient que l'organisation tienne compte des ressources et investissements nécessaires pour mettre en œuvre et opérer un mesure de sécurité par rapport à la valeur métier réalisée. Voir l'ISO/IEC TR 27016 pour les recommandations sur les décisions concernant les investissements dans un SMSI et les conséquences économiques de ces décisions dans le contexte d'exigences concurrentes en matière de ressources.

Il convient qu'il y ait un équilibre entre les ressources déployées pour mettre en œuvre les mesures de sécurité et l'impact métier possible résultant des incidents de sécurité en l'absence de ces mesures de sécurité. Il convient que les résultats de l'appréciation du risque aident à guider et à déterminer les actions de gestion appropriées, les priorités pour gérer les risques de sécurité de l'information, et pour mettre en œuvre les mesures de sécurité identifiées comme nécessaires pour protéger contre ces risques.

Certaines mesures de sécurité dans le présent document peuvent être considérées comme des principes de base pour la gestion de la sécurité de l'information et elles sont applicables à la plupart des organisations. Plus d'informations sur la détermination des mesures de sécurité et autres options de traitement du risque peuvent être trouvées dans l'ISO/IEC 27005.

0.5 Élaboration de lignes directrices spécifiques à une organisation

Le présent document peut être considéré comme point de départ pour l'élaboration de lignes directrices spécifiques à une organisation. Toutes les mesures de sécurité et lignes directrices du présent document peuvent ne pas être applicables à toutes les organisations. D'autres mesures de sécurité et lignes directrices ne figurant pas dans le présent document peuvent être nécessaires pour traiter les besoins spécifiques de l'organisation et les risques identifiés. Lors de la rédaction de documents contenant des lignes directrices ou des mesures de sécurité supplémentaires, il peut être utile d'ajouter des références croisées aux articles du présent document en vue d'une consultation ultérieure.

0.6 Considérations relatives au cycle de vie

L'information a un cycle de vie, depuis sa création jusqu'à son élimination. La valeur de l'information et les risques associés peuvent varier au cours de ce cycle de vie (par exemple, une divulgation non autorisée ou le vol des comptes financiers d'une entreprise n'a pas d'impact significatif après la publication de ces informations, mais l'intégrité demeure critique). Par conséquent, l'importance de la sécurité de l'information subsiste à tous les stades.

Les systèmes d'information et autres actifs pertinents pour la sécurité de l'information ont des cycles de vie durant lesquels ils sont pensés, spécifiés, conçus, développés, testés, mis en œuvre, utilisés, maintenus et finalement retirés du service et mis au rebut. Il convient que la sécurité de l'information soit considérée à chaque étape. Les projets de développement de nouveaux systèmes et les changements apportés aux systèmes existants donnent l'occasion d'améliorer les mesures de sécurité tout en prenant en compte les risques de l'organisation et les leçons tirées des incidents.

0.7 Normes internationales associées

Alors que le présent document propose des recommandations portant sur un vaste éventail de mesures de sécurité qui sont communément utilisées dans plusieurs organisations différentes, d'autres documents de la famille ISO/IEC 27000 proposent des conseils complémentaires ou des exigences relatifs à d'autres aspects du processus global de gestion de la sécurité de l'information.

Se reporter à l'ISO/IEC 27000 pour une introduction générale à la fois aux SMSI et à la famille de documents. L'ISO/IEC 27000 fournit un glossaire, définissant la plupart des termes utilisés dans la famille des documents ISO/IEC 27000, et décrit le périmètre et les objectifs de chaque membre de la famille.

Il existe des normes sectorielles qui comportent des mesures de sécurité supplémentaires destinées à traiter des domaines spécifiques (par exemple, l'ISO/IEC 27017 pour les services en nuage, l'ISO/IEC 27701 pour la protection de la vie privée, l'ISO/IEC 27019 pour l'énergie, l'ISO/IEC 27011 pour les organisations de télécommunications et l'ISO 27799 pour la santé). Ces normes figurent dans la Bibliographie et certaines d'entre elles sont référencées dans les recommandations et autres informations des Articles 5 à 8.

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

1 Domaine d'application

Le présent document fournit un ensemble de référence de mesures de sécurité de l'information génériques, y compris des recommandations de mise en œuvre. Le présent document est conçu pour être utilisé par les organisations:

a) dans le contexte d'un système de gestion de la sécurité de l'information (SMSI) selon l'ISO/IEC 27001;

b) pour la mise en œuvre de mesures de sécurité de l'information basées sur les bonnes pratiques reconnues au niveau international;

c) pour l'élaboration des recommandations de gestion de la sécurité de l'information spécifiques à une organisation.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes, définitions et abréviations

3.1 Termes et définitions

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

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1.1
contrôle d'accès
moyens pour assurer que l'accès physique et logique aux *actifs* (3.1.2) est autorisé et limité selon les exigences de sécurité de l'information et métiers

3.1.2
actif
tout ce qui a de la valeur pour l'organisation

Note 1 à l'article: Dans le contexte de la sécurité de l'information, on peut distinguer deux types d'actifs:

— les actifs essentiels:

  — informations;

  — *processus* (3.1.27) et activités métier;

— les actifs support (sur lesquels reposent les actifs essentiels) de tous types, par exemple:

  — matériel;

  — logiciel;

— réseau;

— *personnel* (3.1.20);

— site;

— structure de l'organisation.

3.1.3
attaque
tentative non autorisée, réussie ou non, de détruire, d'altérer, de désactiver, d'accéder à un *actif* (3.1.2) ou toute tentative d'exposer, de voler ou de faire un usage non autorisé d'un *actif* (3.1.2)

3.1.4
authentification
provision d'assurance qu'une caractéristique revendiquée d'une *entité* (3.1.11) est correcte

3.1.5
authenticité
propriété selon laquelle une *entité* (3.1.11) est ce qu'elle revendique être

3.1.6
chaîne de traçabilité
possession démontrable, déplacement, manipulation et emplacement de matériel d'un moment donné à un autre

Note 1 à l'article: La notion de matériel englobe les informations et les autres *actifs* (3.1.2) associés dans le contexte de l'ISO/IEC 27002.

[SOURCE: ISO/IEC 27050-1:2019, 3.1, modifié — Ajout d'une Note 1 à l'article]

3.1.7
informations confidentielles
informations qui ne sont pas destinées à être rendues disponibles ou divulguées à des personnes, des *entités* (3.1.11) ou des *processus* (3.1.27) non autorisés

3.1.8
mesure de sécurité
action qui maintient et/ou modifie un risque

Note 1 à l'article: Un mesure de sécurité du risque inclut, sans toutefois s'y limiter, n'importe quels *processus* (3.1.27), *politique* (3.1.24), dispositif, pratique ou autres conditions et/ou actions qui maintiennent et/ou modifient un risque.

Note 2 à l'article: Un mesure de sécurité du risque n'aboutit pas toujours nécessairement à la modification voulue ou supposée.

[SOURCE: ISO 31000:2018, 3.8, modifié]

3.1.9
perturbation
incident, anticipé ou non, qui entraîne un écart négatif non planifié par rapport à la livraison de produits et à la fourniture de services prévues selon les objectifs d'une organisation

[SOURCE: ISO 22301:2019, 3.10]

3.1.10
terminal final
terminal matériel de technologies de l'information et de la communication (TIC) connecté au réseau

Note 1 à l'article: Un terminal final peut faire référence à des ordinateurs de bureau, des ordinateurs portables, des smartphones, des tablettes, des clients légers, des imprimantes ou autres matériels spécialisés y compris les compteurs intelligents ou les terminaux Internet des Objets (IoT).

3.1.11
entité
élément pertinent aux fins de fonctionnement d'un domaine et qui possède une existence manifestement distincte

Note 1 à l'article: Une entité peut avoir une matérialisation physique ou logique.

EXEMPLE Une personne, une organisation, un dispositif, un groupe d'éléments de cette nature, un abonné humain à un service de télécommunications, une carte SIM, un passeport, une carte d'interface réseau, une application logicielle, un service ou un site web.

[SOURCE: ISO/IEC 24760-1:2019, 3.1.1]

3.1.12
moyen de traitement de l'information
tout système, service ou infrastructure de traitement de l'information, ou le local les abritant

[SOURCE: ISO/IEC 27000:2018, 3.27, modifié — «moyens» a été remplacé par «moyen».]

3.1.13
violation de sécurité de l'information
compromission de la sécurité de l'information qui entraîne la destruction non souhaitée, la perte, l'altération, la divulgation ou l'accès à des informations protégées transmises, stockées ou soumises à un autre traitement

3.1.14
événement de sécurité de l'information
occurrence indiquant une possible *violation de sécurité de l'information* (3.1.13) ou une violation des *mesures de sécurité* (3.1.8)

[SOURCE: ISO/IEC 27035-1:2016, 3.3, modifié — «violation de la sécurité de l'information» a été remplacé par «violation de sécurité de l'information».]

3.1.15
incident de sécurité de l'information
un ou plusieurs *événements de sécurité de l'information* (3.1.14), pouvant porter préjudice aux *actifs* (3.1.2) d'une organisation ou compromettre son fonctionnement

[SOURCE: ISO/IEC 27035-1:2016, 3.4, modifié]

3.1.16
gestion des incidents de sécurité de l'information
exercice d'une approche cohérente et efficace de la prise en charge des *incidents de sécurité de l'information* (3.1.15)

[SOURCE: ISO/IEC 27035-1:2016, 3.5, modifié]

3.1.17
système d'information
ensemble d'applications, services, *actifs* (3.1.2) informationnels ou autres composants permettant de gérer l'information

[SOURCE: ISO/IEC 27000:2018, 3.35]

3.1.18
partie intéressée
partie prenante
personne ou organisation susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité

[SOURCE: ISO/IEC 27000:2018, 3.37]

3.1.19
non-répudiation
capacité à prouver l'occurrence d'un événement ou d'une action revendiqué(e) et des *entités* (3.1.11) qui en sont à l'origine

3.1.20
personnel
personnes effectuant un travail sous le contrôle de l'organisation

Note 1 à l'article: Le concept de personnel inclut les membres de l'organisation, tels que l'organe de gouvernance, la direction, les employés, le personnel temporaire, les sous-traitants et les bénévoles.

3.1.21
données à caractère personnel
DCP
toute information qui (a) peut être utilisée pour établir un lien entre les informations et la personne physique à laquelle ces informations se rapportent, ou qui (b) est ou peut être associée directement ou indirectement à une personne physique

Note 1 à l'article: La «personne physique» référencée dans la définition est la *personne concernée* (3.1.22). Pour déterminer si une personne concernée est identifiable, il convient de tenir compte de tous les moyens pouvant être raisonnablement utilisés par la partie prenante en matière de protection de la vie privée qui détient les données, ou par toute autre partie, afin d'établir le lien entre l'ensemble de DCP et la personne physique.

[SOURCE: ISO/IEC 29100:2011/Amd.1:2018, 2.9]

3.1.22
personne concernée
personne physique à qui se rapportent les *données à caractère personnel (DCP)* (3.1.21)

Note 1 à l'article: Selon la juridiction et la loi applicable en matière de protection des données et de la vie privée, le terme «sujet des données» peut également être employé en lieu et place de «personne concernée».

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.1.23
sous-traitant de DCP
partie prenante en matière de protection de la vie privée qui traite des *données à caractère personnel (DCP)* (3.1.21) pour le compte d'un responsable de traitement de DCP et conformément à ses instructions

[SOURCE: ISO/IEC 29100:2011, 2.12]

3.1.24
politique
intentions et orientations d'une organisation telles que formalisées par sa direction

[SOURCE: ISO/IEC 27000:2018, 3.53]

3.1.25
étude d'impact sur la vie privée
PIA
processus (3.1.27) global visant à identifier, analyser, évaluer, consulter, communiquer et planifier le traitement des impacts potentiels sur la vie privée au regard du traitement des *données à caractère personnel (DCP)* (3.1.21), dans le cadre plus large du système de management des risques d'une organisation

[SOURCE: ISO/IEC 29134:2017, 3.7, modifié — « évaluation » remplacé par « étude ». Suppression de la note 1 à l'article]

3.1.26
procédure
manière spécifiée d'effectuer une activité ou un *processus* (3.1.27)

[SOURCE: ISO 30000:2009, 3.12]

3.1.27
processus
ensemble d'activités corrélées ou en interaction qui utilise des éléments d'entrée pour produire un résultat

[SOURCE: ISO 9000:2015, 3.4.1, modifié — Suppression des notes à l'article]

3.1.28
enregistrement
informations créées, reçues et préservées comme preuve et *actif* (3.1.2) par une personne physique ou morale dans l'exercice de ses obligations légales ou la conduite des opérations liées à son activité

Note 1 à l'article: Dans ce contexte, les obligations légales comprennent toutes les exigences légales, statutaires, réglementaires et contractuelles.

[SOURCE: ISO 15489-1:2016, 3.14, modifié — Ajout d'une note 1 à l'article]

3.1.29
objectif de point de reprise
OPR
moment auquel les données doivent être rétablies suite à une *perturbation* (3.1.9)

[SOURCE: ISO/IEC 27031:2011, 3.12]

3.1.30
délai de reprise
DR

période au cours de laquelle les niveaux minimum de service et/ou produits, ainsi que les systèmes, applications ou fonctions de soutien, doivent être rétablis suite une *perturbation* (3.1.9)

[SOURCE: ISO/IEC 27031:2011, 3.13]

3.1.31
fiabilité
propriété relative à la cohérence du comportement et des résultats visés

3.1.32
règle
principe admis ou instruction formulant les attentes de l'organisation sur ce qui est nécessaire de faire, ce qui est autorisé ou ce qui ne l'est pas

Note 1 à l'article: Les règles peuvent être exprimées de façon formelle dans des *politiques spécifiques à une thématique* (3.1.35) ainsi que dans d'autres types de documents.

3.1.33
information sensible
information qui nécessite d'être protégée contre l'indisponibilité, l'accès non autorisé, la modification ou la divulgation publique en raison des effets négatifs possibles sur une personne, une organisation, la sécurité nationale ou la sécurité publique

3.1.34
menace
cause potentielle d'un incident indésirable, qui peut nuire à un système ou à une organisation

[SOURCE: ISO/IEC 27000:2018, 3.74]