Norme internationale

ISO/IEC 27031

Deuxième édition
2025-05

Cybersécurité — Préparation des technologies de l'information et de la communication pour la continuité d'activité

Cybersecurity — Information and communication technology readiness for business continuity

Numéro de référence
ISO/IEC 27031:2025(fr)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
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'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

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 deuxième édition annule et remplace la première édition (ISO/IEC 27031:2011), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— la structure du document a été modifiée;

— le domaine d'application a été modifié pour clarification;

— un contenu technique a été ajouté en 6.4, 6.5, 6.6, 9.2 et 10.1.5.

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

Les technologies de l'information et de la communication (TIC) sont devenues, au fil des années, partie intégrante de nombreuses activités au sein des infrastructures critiques dans tous les secteurs d'activité organisationnels, qu'ils soient publics ou privés. Le développement à grande échelle de l'internet et d'autres services de mise en réseaux électroniques, ainsi que les capacités des systèmes et applications, a également eu pour résultat que les organisations sont plus dépendantes d'infrastructures TIC fiables, sécurisées et protégées.

Entre-temps, la nécessité d'un management de la continuité d'activité (MCA), y compris la préparation aux incidents, la planification de la reprise après un sinistre, et la réponse et la gestion des urgences, a été reconnue et soutenue avec le développement et l'approbation de domaines spécifiques de connaissances, d'expertise, et de normes, y compris l'ISO 22313.

Les défaillances des services TIC, y compris celles provoquées par des problèmes liés à la sécurité, tels que la violation de systèmes et les infections par des logiciels malfaisants, influent sur la continuité des opérations Métier. Ainsi, la gestion des TIC et le management de la continuité associée, ainsi que d'autres aspects liés à la sécurité, constituent un élément clé des exigences en matière de continuité d'activité. De plus, dans la majorité des cas, les processus et activités critiques exigeant une continuité d'activité dépendent habituellement des TIC. Cette dépendance signifie que des perturbations des TIC peuvent représenter des risques stratégiques pour la renommée de l'organisation et sa capacité d'action.

Du fait de la prédominance croissante des services TIC basés sur l'internet (services TIC en nuage), la nature de la capacité de préparation a changé, passant d'une dépendance aux processus internes à une dépendance à la qualité et à la robustesse des services fournis par d'autres organisations et aux relations professionnelles avec ces organisations.

Pour de nombreuses organisations, la préparation des TIC est un composant essentiel de la mise en œuvre d'un processus de management de la continuité d'activité et de management de la sécurité de l'information.

Un système MCA efficace dépend ainsi fréquemment d'une préparation efficace des TIC afin de s'assurer que les objectifs d'une organisation peuvent continuer à être satisfaits pendant les perturbations. Cet élément est particulièrement important dans la mesure où les conséquences de perturbations des TIC présentent souvent l'inconvénient supplémentaire d'être invisibles ou difficiles à déceler.

Pour pouvoir réaliser une préparation des TIC de façon à garantir la continuité de son activité (PTCA), il convient qu'une organisation mette en place un processus systématique de prévention, prévision et gestion des perturbations et des incidents liés aux TIC, susceptibles de perturber les services qui leur sont associés. Il est possible d'y parvenir en coordonnant la PTCA avec les processus de sécurité de l'information et de MCA. De cette manière, la PTCA soutient le MCA en s'assurant que les services TIC peuvent être restaurés aux niveaux prédéterminés dans les délais requis et définis par l'organisation.

Lorsqu'une organisation utilise des normes pertinentes en matière de sécurité de l'information et de continuité d'activité, il convient que la mise en place d'une PTCA prenne de préférence en considération les processus existants ou prévus associés à ces normes. Cette association peut prendre en charge l'établissement d'une PTCA, et éviter toute redondance éventuelle de processus pour l'organisation.

Le présent document décrit les concepts et principes de préparation des TIC pour la continuité d'activité (PTCA), et fournit un cadre de méthodes et processus destinés à identifier et spécifier les aspects permettant d'améliorer la préparation des TIC, et ce, de manière à assurer la continuité d'activité d'une organisation.

Le présent document complète les mesures de sécurité de l'information relatives à la continuité d'activité dans l'ISO/IEC 27002. Il soutient également le processus de management des risques liés à la sécurité de l'information spécifié dans l'ISO/IEC 27005.

Sur la base des objectifs de préparation des TIC, le présent document étend également les pratiques de gestion des incidents de sécurité de l'information à la planification, à la formation et à l'exploitation de la préparation des TIC.