INDICE

PREMESSA CEN

Il presente documento (EN ISO 22301:2019) è stato elaborato dal Comitato Tecnico ISO/TC 292 “Security and resilience” in collaborazione con il Comitato Tecnico CEN/TC 391 “Societal and Citizen Security”, la cui segreteria è affidata all’AFNOR.

Alla presente norma europea deve essere attribuito lo status di norma nazionale, o mediante pubblicazione di un testo identico o mediante notifica di adozione, al più tardi entro maggio 2020, e le norme nazionali in contrasto devono essere ritirate al più tardi entro maggio 2020.

Si richiama l’attenzione alla possibilità che alcuni degli elementi del presente documento possano essere oggetto di brevetti. Il CEN (e/o il CENELEC) non deve(devono) essere ritenuto(i) responsabile(i) di avere citato tali brevetti.

Il presente documento sostituisce la EN ISO 22301:2014.

In conformità alle Regole Comuni CEN/CENELEC, gli enti nazionali di normazione dei seguenti Paesi sono tenuti a recepire la presente norma europea: Austria, Belgio, Bulgaria, Cipro, Croazia, Danimarca, Estonia, Finlandia, Francia, Germania, Grecia, Irlanda, Islanda, Italia, Lettonia, Lituania, Lussemburgo, Malta, Norvegia, Paesi Bassi, Polonia, Portogallo, Regno Unito, Repubblica Ceca, Repubblica di Macedonia del Nord, Romania, Serbia, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Turchia e Ungheria.

NOTIFICA DI ADOZIONE

Il testo della ISO 22301:2019 è stato approvato dal CEN come EN ISO 22301:2019 senza alcuna modifica.

PREMESSA ISO

L'ISO (Organizzazione Internazionale di Normazione) è la federazione mondiale degli organismi di normazione nazionali (membri ISO). L'attività di stesura delle norme internazionali è svolta generalmente attraverso comitati tecnici ISO. Ogni organismo membro interessato ad un argomento per il quale è stato istituito un comitato tecnico ha il diritto di essere rappresentato in tale comitato. Anche le organizzazioni internazionali, governative e non-governative, in collaborazione con l'ISO, partecipano ai suddetti lavori. L'ISO collabora strettamente con la Commissione Elettrotecnica Internazionale (IEC) su tutti gli argomenti della normazione elettrotecnica.

Le procedure seguite per sviluppare il presente documento, unitamente a quelle seguite per il suo successivo aggiornamento, sono descritte nelle Direttive ISO/IEC, Parte 1. Inoltre si dovrebbe prestare attenzione ai diversi criteri di approvazione necessari per i diversi tipi di documenti ISO. Il presente documento è stato redatto in conformità alle regole editoriali contenute nelle Direttive ISO/IEC, Parte 2. (vedere: www.iso.org/directives).

Si richiama l'attenzione sulla possibilità che alcuni degli elementi del presente documento possano essere oggetto di brevetti. L'ISO non deve essere ritenuto responsabile di aver citato alcuni o tutti questi brevetti. I dettagli sui brevetti identificati durante lo sviluppo del documento sono indicati nell'Introduzione e/o nell'elenco ISO delle dichiarazioni di brevetto ricevute (vedere www.iso.org/patents).

Qualsiasi denominazione commerciale utilizzata nel presente documento costituisce un'informazione fornita a supporto degli utenti e non costituisce un'approvazione.

Per una spiegazione sulla natura volontaria delle norme, sul significato di termini specifici ISO e delle espressioni relative alla valutazione di conformità, nonché informazioni sull'osservanza dell'ISO ai principi dell'Organizzazione Mondiale del Commercio (WTO) nell'ambito delle barriere tecniche per il commercio (TBT) vedere il seguente URL: www.iso.org/iso/foreword.html.

Il presente documento è stato elaborato dal comitato tecnico ISO/TC 292, Security and resilience.

La presente seconda edizione annulla e sostituisce la prima edizione (ISO 22301:2012), che è stata tecnicamente revisionata. Le modifiche principali rispetto all'edizione precedente sono le seguenti:

- sono stati applicati i requisiti dell'ISO relativi alle norme sui sistemi di gestione, sviluppati dal 2012;
- i requisiti sono stati chiariti, senza aggiungerne di nuovi;
- i requisiti specifici della disciplina “continuità operativa” rientrano ora quasi interamente nel punto 8;
- il punto 8 è stato ristrutturato per fornire una comprensione più chiara dei requisiti chiave;
- un certo numero di termini specifici della disciplina per la continuità operativa è stato modificato per migliorarne la chiarezza e per riflettere il pensiero attuale.

Qualsiasi riscontro o quesito relativo al presente documento dovrebbe essere indirizzato all'organismo di normazione nazionale dell'utilizzatore. Un elenco completo di tali organismi è disponibile all'indirizzo: www.iso.org/members.html.

INTRODUZIONE

0.1 Generalità

Il presente documento specifica la struttura e i requisiti per l'implementazione*) e il mantenimento di un sistema di gestione per la continuità operativa (Business Continuity Management System - BCMS) che sviluppa la continuità operativa in base alla quantità e al tipo di impatto che l'organizzazione può o meno accettare in seguito a un'interruzione.

I risultati del mantenimento di un BCMS sono determinati dai requisiti legali, regolamentari, organizzativi e di settore dell'organizzazione, dai prodotti e servizi forniti, dai processi impiegati, dalle dimensioni e dalla struttura dell'organizzazione e dai requisiti delle parti interessate.

Un BCMS sottolinea l'importanza di:

- comprendere le esigenze dell'organizzazione e la necessità di stabilire politiche e obiettivi per la continuità operativa;
- gestire e mantenere processi, capacità e strutture di risposta per garantire che l'organizzazione sopravviva a interruzioni;
- monitorare e riesaminare le prestazioni e l'efficacia del BCMS;
- il miglioramento continuo basato su misure qualitative e quantitative.

Un BCMS, come qualsiasi altro sistema di gestione, include i seguenti componenti:

a) una politica;
b) persone competenti con responsabilità definite;
c) processi gestionali relativi a:
    1) politica;
    2) pianificazione;
    3) attuazione e funzionamento;
    4) valutazione delle prestazioni;
    5) riesame di direzione;
    6) miglioramento continuo;
d) informazioni documentate a supporto del controllo operativo e che consentano la valutazione delle prestazioni.

0.2 Vantaggi di un sistema di gestione per la continuità operativa

Lo scopo di un BCMS è di preparare, fornire e mantenere controlli e funzionalità per una gestione della capacità complessiva dell'organizzazione di continuare a operare durante le interruzioni. Per raggiungere questo obiettivo, l'organizzazione:

a) dal punto di vista commerciale:
    1) supporta i propri obiettivi strategici;
    2) crea un vantaggio competitivo;
    3) protegge e migliora la propria reputazione e credibilità;
    4) contribuisce alla resilienza organizzativa;
b) dal punto di vista finanziario:
    1) riduce l'esposizione legale e finanziaria;
    2) riduce i costi diretti e indiretti delle interruzioni;
c) dal punto di vista delle parti interessate:
    1) protegge l'incolumità degli individui, le proprietà e l'ambiente;
    2) considera le aspettative delle parti interessate;
    3) Ispira fiducia nella capacità dell'organizzazione di avere successo;

*) Nota nazionale - In questo contesto il termine implementare assume il significato di concepire e mettere in atto.

d) dal punto di vista dei processi interni:

1) migliora la propria capacità di rimanere efficace durante le interruzioni;
2) dimostra un controllo proattivo dei rischi in modo efficace ed efficiente;
3) affronta le vulnerabilità operative.

0.3 Ciclo Plan-Do-Check-Act (PDCA)

Il presente documento applica il ciclo *Plan* (stabilire), *Do* (attuare e gestire), *Check* (monitorare e riesaminare) e *Act* (mantenere e migliorare) (PDCA) per attuare, mantenere e migliorare continuamente l'efficacia del BCMS di un'organizzazione.

Questo garantisce un certo grado di coerenza con le altre norme dei sistemi di gestione, come ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO/IEC 27001 e ISO 28000, supportando in tal modo l'attuazione e il funzionamento coerenti e integrati con i relativi sistemi di gestione.

In conformità con il ciclo PDCA, i punti da 4 a 10 riguardano i seguenti componenti.

- Il punto 4 introduce i requisiti necessari per stabilire il contesto del BCMS applicabile all'organizzazione, nonché le esigenze, i requisiti e il campo di applicazione.
- Il punto 5 riassume i requisiti specifici del ruolo dell'alta direzione nel BCMS e come la leadership articola le proprie aspettative per l'organizzazione attraverso una dichiarazione di policy.
- Il punto 6 descrive i requisiti per stabilire obiettivi strategici e i principi guida per il BCMS nel suo insieme.
- Il punto 7 supporta le operazioni BCMS atte a stabilire competenza e comunicazione su base ricorrente/quando necessario con le parti interessate, mentre documenta, controlla, mantiene e conserva le informazioni documentate richieste.
- Il punto 8 definisce le esigenze per la continuità operativa, determina come affrontarle e sviluppa procedure per gestire l'organizzazione durante un'interruzione.
- Il punto 9 riassume i requisiti necessari per misurare le prestazioni relative alla continuità operativa, la conformità BCMS al presente documento e condurre il riesame di direzione.
- Il punto 10 identifica e agisce in merito alla non conformità BCMS e al miglioramento continuo attraverso azioni correttive.

0.5 Contenuto del presente documento

Il presente documento è conforme ai requisiti ISO per le norme sui sistemi di gestione. Questi requisiti comprendono una struttura di alto livello, un testo di base e termini comuni identici con le definizioni di base, ideati a beneficio degli utilizzatori che mettono in atto diverse norme ISO sui sistemi di gestione.

Il presente documento non include requisiti specifici di altri sistemi di gestione, sebbene i suoi elementi possano essere allineati o integrati con quelli di altri sistemi di gestione.

Il presente documento contiene requisiti che possono essere utilizzati da un'organizzazione per attuare un BCMS e valutare la conformità. Un'organizzazione che desidera dimostrare la conformità al presente documento può farlo:

- effettuando una auto-valutazione e auto-dichiarazione, oppure
- richiedendo la conferma della propria conformità ad altri soggetti che hanno un interesse nell'organizzazione stessa, come per esempio i clienti, oppure
- richiedendo ad una parte esterna rispetto all'organizzazione la conferma della propria auto-dichiarazione, oppure
- richiedendo la certificazione/registrazione del proprio BCMS da parte di una organizzazione esterna.

I punti da 1 a 3 nel presente documento definiscono lo scopo e il campo di applicazione, i riferimenti normativi e i termini e le definizioni che si applicano all'utilizzo del presente documento. I punti da 4 a 10 contengono i requisiti da utilizzare per valutare la conformità al presente documento.

Nel presente documento sono utilizzate le seguenti forme verbali:

a) "deve" indica un requisito;

b) "dovrebbe" indica una raccomandazione;

c) "può"[**)] (may) indica un permesso;

d) “può” (can) indica una possibilità o una capacità.

Le informazioni riportate come "NOTA" sono una guida per comprendere o per chiarire il requisito correlato. Le “Note” utilizzate nel punto 3 forniscono informazioni aggiuntive che integrano i dati terminologici e possono contenere disposizioni relative all'utilizzo di un termine.

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento specifica i requisiti per attuare, mantenere e migliorare un sistema di gestione per proteggere l’organizzazione da interruzioni, ridurre la probabilità che si verifichino, prepararsi, rispondere e riprendersi dalle stesse quando accadono.

I requisiti specificati nel presente documento sono generici e sono destinati ad essere applicabili a tutte le organizzazioni, o a parti di esse, indipendentemente dal tipo, dalle dimensioni e dalla natura dell'organizzazione. La portata dell'applicazione di questi requisiti dipende dall'ambiente operativo e dalla complessità dell'organizzazione.

Il presente documento è applicabile a tutti i tipi e dimensioni di organizzazioni che:

a) attuano, mantengono e migliorano un BCMS;

b) cercano di garantire la conformità con la politica per la continuità operativa dichiarata;

c) hanno la necessità di essere in grado di continuare a fornire prodotti e servizi ad una capacità predefinita accettabile durante un'interruzione;

d) cercano di migliorare la loro resilienza attraverso l'effettiva applicazione del BCMS.

Il presente documento può essere utilizzato per valutare la capacità di un'organizzazione di soddisfare le proprie esigenze e obblighi per la continuità operativa.

2 RIFERIMENTI NORMATIVI

Nel testo si fa riferimento ai seguenti documenti in modo tale che il loro contenuto, in tutto o in parte, costituisca i requisiti per il presente documento. Per quanto riguarda i riferimenti datati, si applica esclusivamente l’edizione citata. Per i riferimenti non datati vale l’ultima edizione del documento a cui si fa riferimento (compresi gli aggiornamenti).

ISO 22300 Security and resilience - Vocabulary

3 TERMINI E DEFINIZIONI

Ai fini del presente documento, si applicano i termini e le definizioni di cui alla ISO 22300 e i termini e le definizioni seguenti.

Per l’utilizzo in ambito normativo l’ISO e l’IEC dispongono di banche dati terminologiche ai seguenti indirizzi:

- ISO Online browsing platform: disponibile all’indirizzo http://www.iso.org/obp
- IEC Electropedia: disponibilie all’indirizzo http://www.electropedia.org/

Nota I termini e le definizioni riportati qui di seguito sostituiscono quelli della ISO 22300:2018.

**) Nota Nazionale - Nella presente norma è utilizzato lo stesso verbo per la traduzione in italiano di "may" e "can". La diversa accezione è desumibile dal contesto relativo alla specifica frase.