INDICE

PREMESSA CEN

Il testo della ISO/IEC 27001:2022 è stato elaborato dal Comitato Tecnico ISO/IEC JTC 1 “Information technology” dell’Organizzazione Internazionale di Normazione (ISO) ed è stato ripreso come EN ISO/IEC 27001:2023 dal Comitato Tecnico CEN-CENELEC/JTC 13 "Cybersecurity and Data Protection" la cui segreteria è affidata al DIN.

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 gennaio 2024, e le norme nazionali in contrasto devono essere ritirate al più tardi entro gennaio 2024.

Si richiama l’attenzione alla possibilità che alcuni degli elementi del presente documento possano essere oggetto di brevetti. Il CEN-CENELEC non deve essere ritenuto responsabile di avere citato tali brevetti.

Il presente documento sostituisce la EN ISO/IEC 27001:2017.

Qualsiasi commento o richiesta sul presente documento dovrebbe essere rivolta al proprio ente di normazione nazionale. Una lista completa di tali enti è disponibile nei siti web del CEN e del CENELEC.

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 Nord della Macedonia, Romania, Serbia, Slovacchia, Slovenia, Spagna, Svezia, Svizzera, Turchia e Ungheria.

NOTIFICA DI ADOZIONE

Il testo della ISO/IEC 27001:2022 è stato approvato dal CEN-CENELEC come EN ISO/IEC 27001:2023 senza alcuna modifica.

PREMESSA ISO

L'ISO (l'Organizzazione Internazionale di Normazione) e l'IEC (la Commissione Elettrotecnica Internazionale) costituiscono il sistema specializzato per la standardizzazione mondiale. Gli organismi nazionali che sono membri dell'ISO o dell'IEC partecipano allo sviluppo delle norme internazionali attraverso comitati tecnici istituiti dalla rispettiva organizzazione per occuparsi di particolari campi di attività tecnica. I comitati tecnici ISO e IEC collaborano in settori di reciproco interesse. Ai lavori partecipano anche altre organizzazioni internazionali, governative e non governative, in collegamento con ISO e IEC.

Le procedure utilizzate per lo sviluppo di questo documento e quelle previste per il suo ulteriore mantenimento sono descritte nelle Direttive ISO/IEC, Parte 1. In particolare, vanno notati i diversi criteri di approvazione necessari per i diversi tipi di documento. Questo documento è stato redatto in conformità con le regole editoriali delle Direttive ISO/IEC, Parte 2 (vedere www.iso.org/directives o www.iec.ch/members_experts/refdocs).

Si richiama l'attenzione sulla possibilità che alcuni elementi del presente documento possano essere oggetto di diritti di brevetto. ISO e IEC non saranno ritenuti responsabili dell'identificazione di uno o di tutti questi diritti di brevetto. I dettagli di eventuali diritti di brevetto identificati durante lo sviluppo del documento saranno nell'Introduzione e/o nell'elenco ISO delle dichiarazioni di brevetto ricevute (vedere www.iso.org/patents) o nell'elenco IEC delle dichiarazioni di brevetto ricevute (vedere https://patents.iec.ch).

Qualsiasi nome commerciale utilizzato in questo documento è un'informazione fornita per comodità degli utenti e non costituisce un'approvazione.

Per una spiegazione della natura volontaria delle norme, del significato dei termini e delle espressioni specifici dell'ISO relativi alla valutazione della conformità, nonché per informazioni sull'adesione dell'ISO ai principi relativi agli ostacoli tecnici al commercio (Technical Barriers to Trade, TBT) dell'Organizzazione mondiale del commercio (World Trade Organization, WTO), vedere www.iso.org/iso/foreword.html. Nella IEC, vedere www.iec.ch/understanding-standards.

Questo documento è stato preparato dal Comitato Tecnico Congiunto ISO/IEC JTC 1, *Tecnologie Informatiche*, Sottocomitato SC 27, *Sicurezza delle informazioni, cybersecurity e protezione della privacy*.

Questa terza edizione annulla e sostituisce la seconda edizione (UNI CEI EN ISO/IEC 27001:2017), che è stata tecnicamente aggiornata. Incorpora anche la Rettifica Tecnica ISO/IEC 27001:2013/Cor 1:2014 e ISO/IEC 27001:2013/Cor 2:2015.

I cambiamenti principali sono i seguenti:

- il testo è stato allineato con la struttura armonizzata per i sistemi di gestione e con la UNI CEI EN ISO/IEC 27002:2023.

Eventuali commenti o domande su questo documento dovrebbero essere indirizzati all'organismo di normazione nazionale dell'utilizzatore. Un elenco completo di questi organismi può essere trovato su www.iso.org/members.html e www.iec.ch/national-committees.

INTRODUZIONE

0.1 Generalità

Il presente documento è stato elaborato allo scopo di fornire i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni. L'adozione di un sistema di gestione per la sicurezza delle informazioni è una decisione strategica per un'organizzazione. Stabilire e attuare un sistema di gestione per la sicurezza delle informazioni di un'organizzazione sono influenzati dalle sue necessità e obiettivi, dai suoi requisiti di sicurezza, dai suoi processi organizzativi e dalla sua dimensione e struttura. È previsto che tutti questi fattori cambino nel tempo.

Il sistema di gestione per la sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità dalle informazioni mediante l'applicazione di un processo di gestione del rischio e dà fiducia alle parti interessate sull'adeguatezza della gestione dei rischi.

È importante che il sistema di gestione per la sicurezza delle informazioni sia parte integrante dei processi e della struttura gestionale complessiva dell'organizzazione e che la sicurezza delle informazioni sia considerata nella progettazione dei processi, dei sistemi informativi e dei controlli. Ci si attende che un sistema di gestione per la sicurezza delle informazioni sia commisurato alle necessità dell'organizzazione.

Il presente documento può essere utilizzato da parti interne ed esterne al fine di valutare la capacità di un'organizzazione di soddisfare i propri requisiti relativi alla sicurezza delle informazioni.

L'ordine con cui sono presentati i requisiti nella presente norma internazionale non riflettono il loro livello di importanza, né implica un ordine con cui devono essere attuati. Gli elementi delle liste sono numerati solo per finalità di referenziazione.

La EN ISO/IEC 27000 presenta una visione d'insieme e il vocabolario dei sistemi di gestione per la sicurezza delle informazioni, citando la famiglia di norme relative ai sistemi di gestione per la sicurezza delle informazioni (tra cui la ISO/IEC 27003[2], la ISO/IEC 27004[3] e la ISO/IEC 27005[4]), con i termini e le definizioni correlati.

0.2 Compatibilità con altre norme relative ai sistemi di gestione

Il presente documento utilizza la struttura ad alto livello, gli stessi titoli per i punti, il testo identico, i termini comuni e le definizioni fondamentali definite nell'Annex SL delle ISO/IEC Directives, Part 1, Consolidated ISO Supplement, e mantiene quindi la compatibilità con le altre norme relative ai sistemi di gestione che hanno adottato l'Annex SL.

L'approccio comune definito dall'Annex SL è utile a quelle organizzazioni che scelgono di realizzare un unico sistema di gestione che soddisfi i requisiti di due o più norme relative ai sistemi di gestione.

1 SCOPO E CAMPO DI APPLICAZIONE

Il presente documento specifica i requisiti per stabilire, attuare, mantenere e migliorare in modo continuo un sistema di gestione per la sicurezza delle informazioni nel contesto di un'organizzazione. Il presente documento include anche i requisiti per la valutazione e il trattamento dei rischi relativi alla sicurezza delle informazioni adattati alle necessità dell'organizzazione. I requisiti stabiliti dal presente documento sono di carattere generale e predisposti per essere applicabili a tutte le organizzazioni, indipendentemente dalla loro tipologia, dimensione e natura. L'esclusione di qualunque requisito specificato nei punti dal 4 al 10 non è accettabile quando un'organizzazione dichiara la sua conformità al presente documento.

2 RIFERIMENTI NORMATIVI

I seguenti documenti, in tutto o in parte, sono richiamati con carattere normativo nel presente documento e sono indispensabili per la sua applicazione. 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/IEC 27000 Information technology (IT) – Tecniche di sicurezza – Sistemi di gestione per la sicurezza delle informazioni – Visione d'insieme e vocabolario

3 TERMINI E DEFINIZIONI

Ai fini del presente documento si applicano i termini e le definizioni specificati dalla ISO/IEC 27000.

ISO e IEC mantengono dei database di termini utilizzati nella normazione e reperibili ai seguenti indirizzi:

- ISO Online browsing platform: disponibile all'indirizzo https://www.iso.org/obp
- IEC Electropedia: disponibile all'indirizzo https://www.electropedia.org/

4 CONTESTO DELL'ORGANIZZAZIONE

4.1 Comprendere l'organizzazione e il suo contesto

L'organizzazione deve individuare i fattori esterni e interni che sono rilevanti per le sue finalità e che influenzano la sua capacità di conseguire i risultati attesi per il proprio sistema di gestione per la sicurezza delle informazioni.

Nota La determinazione di questi fattori fa riferimento alla definizione del contesto esterno e interno dell'organizzazione considerato al punto 5.4.1 della ISO 31000:2018[5].

4.2 Comprendere le esigenze e le aspettative delle parti interessate

L'organizzazione deve individuare:

a) le parti interessate rilevanti per il sistema di gestione per la sicurezza delle informazioni;

b) i requisiti pertinenti di tali parti interessate;

c) quali di questi requisiti si vogliono gestire attraverso il sistema di gestione per la sicurezza delle informazioni.

Nota I requisiti delle parti interessate possono includere requisiti cogenti*) e obblighi contrattuali.

4.3 Determinare il campo di applicazione del sistema di gestione per la sicurezza delle informazioni

L'organizzazione deve determinare i confini e l'applicabilità del sistema di gestione per la sicurezza delle informazioni per stabilirne il campo di applicazione.

Nello stabilire il campo di applicazione, l'organizzazione deve considerare:

a) i fattori esterni e interni di cui al punto 4.1;

b) i requisiti di cui al punto 4.2;

c) le interfacce e le interdipendenze tra le attività svolte dall'organizzazione, e quelle svolte da altre organizzazioni.

Il campo di applicazione deve essere disponibile come informazione documentata.

*) Nota nazionale - Per "requisiti cogenti" si intendono, nel seguito, quelli stabiliti da leggi, regolamenti, direttive (requisiti legali) e prescrizioni obbligatorie in genere.