Gestione per la sicurezza delle informazioni, cosa cambia con la nuova ISO/IEC 27001:2022

*La rubrica "**Digital & Law**" è curata da **D&L Net** e offre una lettura delle materie dell'innovazione digitale da una prospettiva che sia in grado di offrire piena padronanza degli strumenti e dei diritti digitali, anche ai non addetti ai lavori. Per consultare tutti gli articoli clicca qui.*

A fine ottobre 2022 è stata pubblicata l'ultima edizione dello standard internazionale ISO/IEC 27001 dal titolo "Information security, cybersecurity and privacy protection – Information security management systems – Requirements".

Lo standard riporta i requisiti per i sistemi di gestione per

la sicurezza delle informazioni e può essere usato per ottenere un certificato di conformità da organismi di certificazione accreditati.

Questa edizione sostituisce la **ISO/IEC 27001:2013** (recepita in Italia come UNI CEI EN ISO/IEC 27001:2017) e in questo articolo sono riportati i principali cambiamenti. Quelli più significativi riguardano i controlli dell'Appendice A, come sarà illustrato nel seguito.

Nei prossimi mesi e anni, altre norme collegate alla ISO/IEC 27001 verranno aggiornate. Tra queste vi sono la ISO/IEC 27017 (sull'uso o l'erogazione di servizi cloud), la ISO/IEC 27018 (sulla gestione della privacy da parte dei fornitori di servizi cloud), la ISO/IEC 27701 (sulla gestione della privacy).

Cosa cambia, ad iniziare dal titolo

Innanzitutto, il titolo precedente era "Information technology – Security techniques – Information security management systems – Requirements" per riflettere il nome del gruppo che mantiene la norma (ISO/IEC JTC 1 SC 27 WG 1). Adesso il gruppo ha cambiato nome per dare, giustamente, **maggiore evidenza del fatto che si occupa sì di sicurezza informatica** (e cybersicurezza), ma anche di sicurezza delle informazioni e di privacy.

Cambiamenti ai requisiti (capitoli dal 4 al 10)

La ISO/IEC 27001 riguarda i sistemi di gestione, per i quali è necessario seguire un modello noto come "high-level structure". Questo modello è stato aggiornato dal 2013 e pertanto la nuova ISO/IEC 27001 ne recepisce i cambiamenti.

Molti di essi sono formali, atti a migliorarne la chiarezza

(per esempio, i paragrafi 9.2 e 9.3 sono stati suddivisi in 2 sottoparagrafi ciascuno, senza però cambiarne il contenuto).

Alcuni cambiamenti più significativi sono:

- aggiunto il punto 4.2.c per esplicitare quali requisiti delle parti interessate sono affrontati dal sistema di gestione per la sicurezza delle informazioni;
- aggiunto il punto 6.3 che richiede che i cambiamenti al sistema di gestione siano pianificati.

Significativo è il consolidamento con la correzione già pubblicata nel 2015, che rende più esplicito il fatto che la Dichiarazione di applicabilità (ossia l'elenco dei controlli attuati e di quelli che si intendono attuare) non deve necessariamente riportare i controlli dell'Appendice A della norma (ossia quelli della ISO/IEC 27002:2022), ma può riportarne altri.

Oggi, quindi, al punto 6.1.3, si esplicita che la lista dei controlli di questa norma non è più "comprensiva" ma è solo una delle "possibili" liste di controlli.

Rimane necessario indicare quali controlli dell'Appendice A sono esclusi. Questo richiede quindi una verifica di completezza dell'elenco dei controlli rispetto all'Appendice A e pertanto molti preferiranno comunque usare questo elenco.

Cambiamenti ai controlli (Appendice A)

L'Appendice A della ISO/IEC 27001:2022 è stata modificata per allinearla alla ISO/IEC 27002:2022. I controlli sono stati ridotti, rispetto all'edizione del 2013, da 114 a 93 e riorganizzati in 4 "temi" al posto dei 14 "punti" precedenti, rimuovendo anche le 33 "categorie di controllo".

I controlli aggiunti rispetto alla precedente edizione sono:

- 5.7 Threat intelligence (raccolta, analisi e uso di informazioni sulle minacce relative alla sicurezza delle informazioni);
- 5.23 sull'uso dei servizi cloud, assente nella precedente edizione in quanto parte del controllo relativo alla catena di fornitura;
- 5.30 sulla prontezza dell'ICT per la continuità operativa, che non aggiunge niente di quanto già presente nella precedente edizione, ma riflette il fatto che i controlli relativi alla continuità operativa sono stati riorganizzati;
- 7.4 Monitoraggio della sicurezza fisica: relativo agli strumenti attivi di controllo della sicurezza fisica (telecamere e allarmi);
- 8.9 sulla sicurezza delle configurazioni (ossia delle impostazioni) di server, dispositivi e applicazioni; questo controllo include l'adozione di tecniche di hardening per i sistemi critici; nella precedente edizione della norma questo controllo era colpevolmente assente;
- 8.10 sulla cancellazione delle informazioni al termine dei tempi di conservazione previsti o al termine del rapporto di lavoro con un cliente; questo controllo era in precedenza solo accennato, mentre erano ben due i controlli relativi alla distruzione o cancellazione dei supporti di memorizzazione;
- 8.11 sull'anonimizzazione e pseudonimizzazione dei dati;
- 8.12 sulla possibilità di usare strumenti DLP (data loss prevention);
- 8.16 sul monitoraggio delle attività, colpevolmente assente dall'edizione precedente;
- 8.23 sui filtri per la navigazione sul web, in precedenza incluso tra i controlli di rete;
- 8.28 sulla codifica sicura, che non aggiunge molto rispetto a quanto già presente nella precedente edizione, ma riflette il fatto che i controlli relativi allo sviluppo sicuro sono stati riorganizzati e

migliorati.

Da segnalare, dalla ISO/IEC 27002:2022, 3 sotto-controlli che potrebbe valere la pena considerare con maggiore attenzione:

- controllo dei visitatori;
- trasferimenti orali delle informazioni;
- requisiti contrattuali dei clienti.

Altri controlli, anche se non nuovi, sono notevolmente cambiati e pertanto sarà necessario analizzarli con attenzione:

- 5.16 sulla gestione delle identità, che amplia il precedente “Registrazione e de-registrazione degli utenti”;
- 8.1 sugli endpoint degli utenti (pc, laptop, tablet, cellulari e smartphone e altri), che sostituisce il precedente “Politica per i dispositivi portatili“, molto più limitato.

Oltre a questi, si richiama ancora l’attenzione alla riorganizzazione dei controlli relativi alla continuità operativa e allo sviluppo sicuro.

Transizione dei certificati

Le regole pubblicate da IAF (l’organismo che controlla gli accordi di mutuo riconoscimento tra organismi di accreditamento membri di IAF, tra cui l’italiano Accredia, che a loro volto controllano gli organismi di certificazione accreditati) richiedono che i certificati ISO/IEC 27001 validi siano tutti basati sulla nuova edizione entro il 31 ottobre 2025.

Si raccomanda alle organizzazioni certificate di prestare attenzione alle comunicazioni che riceveranno in merito dal proprio organismo di certificazione, in modo da pianificare la transizione.

Conclusioni

Come già detto, le modifiche significative sono quelle relative ai controlli di sicurezza dell'Appendice A. Tali modifiche sono poco numerose e pertanto la transizione non dovrebbe essere complessa per le organizzazioni già certificate.

Si segnala che, come riporta anche IAF, la ISO/IEC 27001, anche nella precedente edizione, non richiede di attuare i controlli dell'Appendice A, ma di identificare i controlli necessari e confrontarli con quelli dell'Appendice A. Questo non dovrebbe quindi portare alla "scoperta" di controlli necessari. Se questo dovesse invece accadere, l'organizzazione dovrebbe aggiornare il proprio piano di trattamento del rischio e attuarli, seguendo le procedure del proprio sistema di gestione per la sicurezza delle informazioni.

Gli standard ISO/IEC 27001 e ISO/IEC 27002 per la sicurezza delle informazioni: per approfondire

Non perdere il corso in e-learning per professionisti ed aziende sviluppato da Digital&Law, patrocinato da ANORC Professioni. Il corso si struttura in tre moduli per una durata complessiva di 6 ore:

- Lo standard ISO/IEC 27001:2013
- Lo standard ISO/IEC 27002:2022
- Lo standard ISO/IEC 27701: 2019

https://www.key4biz.it/gestione-per-la-sicurezza-delle-informazioni-cosa-cambia-con-la-nuova-iso-iec-270012022/425892/