

ISO, in vigore i nuovi standard globali per la sicurezza delle informazioni



È stata recentemente pubblicata l'attesa terza edizione della ISO/IEC 27001, intitolata (con l'importante aggiunta delle parole *cybersecurity* e *privacy protection*, assenti nei titoli delle vecchie edizioni) *"Information security, cybersecurity and privacy protection I Information security management systems / Requirements"*.

L'aggiornamento dello standard – inizialmente rilasciato nel 2005 e già varie volte integrato tramite revisioni quinquennali o *technical corrigenda* specifici – ha lo scopo di allineare i requisiti alle nuove esigenze di sicurezza di aziende ed enti istituzionali nei vari Paesi, a prescindere dal segmento di business o dalle finalità perseguite dalle singole organizzazioni.

Come le antecedenti edizioni, la norma s'impone a titolo di riferimento per ogni sistema di gestione per la sicurezza delle informazioni (**SGSI** nell'acronimo italiano, **ISMS** – *Information Security Management System* in inglese) sul piano internazionale.

Gli aspetti salienti della nuova versione

In termini di controlli di sicurezza, la ISO/IEC 27001:2022 ne prevede un numero minore rispetto ai documenti che l'hanno preceduta. Per effetto dell'eliminazione di alcune procedure ritenute ormai superate e dell'integrazione di altre fra loro, i controlli ora richiesti (elencati nell'Appendice A, la parte soggetta alle principali modifiche) sono infatti 93, contro i 114 del 2017; ma sono anche state aggiunte 11 nuove tipologie,

fra cui quelle relative alle attività di *Threat intelligence* e di *Physical security monitoring*.

Oltre a tale dato quantitativo, la revisione ha introdotto il punto 6.3 (dal titolo “Pianificazione dei cambiamenti”) che impone un *planning* più rigoroso per ogni tipo di aggiornamento che possa interessare il sistema di gestione del patrimonio informativo aziendale.

In generale lo standard così ridefinito mira a prevedere valutazioni e *check* di sicurezza meno massivi e più mirati, probabilmente anche in considerazione del proliferare di ambienti digitali ibridi e della crescente pervasività del *Cloud*.

Attestazioni e oneri di *compliance* per le aziende

Dal momento della pubblicazione è stabilito un termine di tre anni – fino al 31 ottobre del 2025 – per adeguarsi alla nuova normativa.

Entro tale periodo le organizzazioni già certificate, al fine di vedersi ufficialmente attribuita una dichiarazione di conformità ai requisiti aggiornati, dovranno rivolgersi a un organismo riconosciuto dall’ente di accreditamento nazionale (che in Italia è rappresentato dall’Ente Unico Accredia, membro del Forum IAF) per sottoporsi all’*audit* di transizione richiesto.

Per chi debba ottenere la prima certificazione il termine è invece fissato in un anno, con scadenza quindi al 31 ottobre 2023.

Certificare la piena adesione agli standard internazionali di sicurezza rappresenta un importante “bollino di qualità”, in particolar modo per le imprese. In tal modo queste ultime possono dimostrare di aver implementato le migliori procedure

di *Risk Assessment* e gestione delle informazioni a tutela della propria continuità operativa, nonché della privacy dei dati di utenti e clienti; così potendo collocarsi a pieno titolo sul mercato globale, garantendosi anche un'effettiva parità di condizioni con i *competitor* di altri Paesi.

A cura della Redazione

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/iso-in-vigore-i-nuovi-standard-globali-per-la-sicurezza-delle-informazioni/>