PERRY JOHNSON REGISTRARS, INC.

ISO 27002: Perché è diversa dalla 27001 e cosa cambia?

La ISO 27001 è una norma internazionalmente riconosciuta per la sicurezza dei dati e la tecnologia, che offre alle aziende di ogni dimensione la certezza di pratiche consolidate per salvaguardare le proprie attività e quelle dei propri clienti. Meno conosciuta è la ISO 27002 - nome che appare sempre più spesso negli ultimi mesi, in seguito all'annuncio di aggiornamenti e modifiche. Cos'è esattamente la 27002, e come incide sulla ISO 27001?

Mentre la ISO 27001 è il cuore fondante della serie di norme ISO 27000, la ISO 27002 è una norma supplementare. La norma è incentrata sui controlli di sicurezza dei dati elencati nell'allegato A della 27001 che le aziende possono scegliere di implementare, e offre consigli su come implementarli al meglio. Tuttavia, mentre la norma ISO 27001 offre semplicemente un elenco di controlli con una breve descrizione, la 27002 approfondisce tutti i controlli: a ciascuno è dedicata almeno una pagina di contenuto!

Se questo livello di dettaglio fosse stato incluso nella ISO 27001, sarebbe diventata inutilmente lunga. Avendo oltre 100 controlli da gestire, è necessario un documento dedicato per rendere giustizia a ognuno di essi, con tutta la profondità e l'ampiezza necessarie. Tuttavia, sebbene ISO 27002 sia ricca di informazioni, non si tratta di una norma certificabile a sé stante; è possibile certificare solo la ISO 27001, mentre la 27002 viene considerata un documento di accompagnamento.

Nell'ambito della ISO 27002:2013, i 114 controlli di sicurezza dei dati sono suddivisi nelle seguenti 14 categorie:

- Politiche sulla sicurezza dei dati
- Sicurezza delle risorse umane
- Controllo degli accessi
- Sicurezza fisica ed ambientale
- Acquisizione, sviluppo e manutenzione del sistema
- Gestione degli incidenti in materia di sicurezza dei dati
- Aspetti legati alla sicurezza dei dati nella gestione della continuità aziendale
- Organizzazione della sicurezza dei dati
- Gestione degli asset
- Crittografia
- Sicurezza delle operazioni
- Sicurezza delle comunicazioni
- Rapporti con i fornitori
- Conformità

Utilizzare sia la ISO 27001 che la 27002 insieme è importantissimo, specialmente se l'organizzazione effettua una valutazione dei rischi per individuare e dare priorità alle minacce legate alla sicurezza dei dati. Non tutti i controlli si applicano a tutte le organizzazioni; il primo passo da compiere è individuare i controlli su cui concentrarsi.

Che cosa cambia nella ISO 27002 tanto da far conoscere la norma al pubblico? Semplicemente, la norma è stata ristrutturata. Rispetto alle 14 sezioni di 114 controlli, la ISO 27002:2022 viene ridotta a 93 controlli suddivisi in 4 sezioni, più 2 allegati:

- Controlli organizzativi (clausola 5)
- Controlli fisici (clausola 7)
- Allegato A - Uso degli accessori
- Controlli sulle persone (clausola 6)
- Controlli tecnologici (clausola 8)
- Allegato B - Corrispondenza con ISO/IEC 27002:2013

Questo riassetto della ISO 27002 implica anche un prossimo aggiornamento della ISO 27001, con riferimenti aggiornati alle nuove sezioni della 27002 e al minor numero di controlli. Quando verrà rilasciata la nuova revisione della ISO 27001, è previsto un periodo di transizione di circa 2-3 anni durante il quale le organizzazioni certificate dovranno adottare la nuova serie di controlli, aggiornando i loro sistemi per adeguarli alla nuova revisione.

Per restare aggiornati sulle novità delle norme ISO 27001 e 27002, iscrivetevi alla mailing list di PJR visitando il nostro sito web: **www.pjritaly.com**! Per saperne di più sui nostri programmi ISMS e sulle risorse gratuite, chiamateci oggi stesso al numero **0823/354874**!