Sicurezza delle informazioni, la nuova ISO/IEC 27001:2022: ecco cosa cambia - Agenda Digitale

A fine ottobre 2022 è stata pubblica l'ultima versione dello standard internazionale ISO/IEC 27001 con i requisiti per i sistemi di gestione per la sicurezza delle informazioni.

Dalla prima versione del 2005 della ISO/IEC 27001 (a sua volta nata dalla BS 7799, la cui prima versione era del 1997), molte cose sono cambiate nel mondo delle discipline che si occupano di proteggere i sistemi informativi e quanto questi supportano, a partire dallo stesso nome che, da sicurezza "informatica", o addirittura "logica", è passato a sicurezza delle "informazioni" per poi essere comunemente ma spesso impropriamente etichettato dal grande pubblico come **cybersecurity.**

La ISO/IEC 27001 ha, da allora, subito **una prima trasformazione significativa** nella sua seconda versione uscita nel 2013, principalmente legata all'introduzione della "high-level structure", oggi comune a tutti i sistemi di gestione pubblicati da ISO. Ora ne è stata pubblicata una nuova, terza versione che, come vedremo nel corso di questo articolo, non ne va a sconvolgere più di tanto la forma o la sostanza, con l'eccezione della parte dei controlli presentati nell'Appendice A.

La dinamica che ha portato a questa terza versione della ISO/IEC 27001 è figlia di una decisione presa nel 2016 in seno al Working Group (WG) 1 di ISO/IEC JTC 1 SC 27, che ha dato i natali alla norma e a quelle ad essa legate, in occasione del voto circa la sua revisione periodica, prevista, come per tutte le norme ISO, ogni 5 anni. In tale occasione si è infatti deciso che la ISO/IEC 27002 avrebbe dovuto essere oggetto di **una revisione significativa** per ammodernarla e rimetterla al passo con i tempi mentre la ISO/IEC 27001 sarebbe stata lasciata sostanzialmente stabile, salvo allinearne la parte dei controlli in Appendice A.

A questa decisione iniziale si sono sovrapposte **riflessioni** spinte da alcuni esperti circa la modifica del meccanismo dello "statement of applicability" e gli aggiornamenti periodici della "high-level structure" portati avanti dalla stessa ISO, innescando un balletto di indecisione su come affrontare al meglio i lavori e che ha portato, diversamente a quanto accadde in modo perfettamente sincrono nel 2013, ad avere nel 2022 un'uscita distanziata di oltre 6 mesi delle nuove ISO/IEC 27002 e 27001.

La nuova versione della ISO/IEC 27001 risulta essere in sintesi:

- allineata alla nuova "high-level structure" (capitoli da 1 a 10);
- allineata alla nuova ISO/IEC 27002 (appendice A);
- inclusiva dei due "technical corrigendum" pubblicati nel 2014 e nel 2015;
- aggiornata nel punto 6.1.3 dove viene richiamata l'appendice A.

I cambiamenti apportati per allinearsi alla nuova HLS

I cambiamenti apportati per allineamento alla nuova "high-level structure" sono per lo più formali, come ad esempio:

- la **sostituzione** di "la presente norma internazionale" con "il presente documento";
- **l'aggiunta** di paragrafi (solo come titoli, non come contenuti) nei punti 9.2 (audit interno) e 9.3 (riesame della direzione);
- **l'inversione** dei punti 10.1 (miglioramento continuo) e 10.2 (non conformità e azioni correttive).

Ci sono tuttavia **alcuni cambiamenti che avranno un impatto sui sistemi di gestione per la sicurezza delle informazioni esistenti:**

- **Nel punto 4** (contesto dell'organizzazione) si aggiunge un punto 4.2 c) che richiede non solo di individuare i requisiti delle parti interessate ma anche di individuare quali di essi saranno affrontati dal sistema di gestione.
- **Nel punto 4.4,** che richiede di attuare il sistema di gestione per la sicurezza delle informazioni nel suo complesso, sono stati espressamente citati i processi necessari al sistema di gestione e le loro interazioni, prima erano dati per sottintesi.
- **Gli obiettivi richiamati al punto 6.2** dovranno ora essere anche monitorati per effetto dell'aggiunta del punto d).
- **Tutto il punto 6.3** (pianificazione dei cambiamenti) viene introdotto per la prima volta e richiede che i cambiamenti al sistema di gestione siano sempre portati a termine in modo pianificato. Al punto 7.4 (comunicazione), sono stati rimossi i due sottopunti d) ed e) relativi a chi deve comunicare e tramite quale processo, rimpiazzandoli con un nuovo sottopunto d) su come si deve comunicare.

Per effetto della revisione della ISO/IEC 27002, invece, 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, oltre a rimuovere il riferimento agli obiettivi di

I technical corrigendum del 2014 e 2015

La ISO/IEC 27001:2022 incorpora le **due correzioni** (technical corrigendum) pubblicate nel 2014 e 2015.

La prima correzione derivava da una correzione apportata alla ISO/IEC 27002:2013 e quindi oggi non più presente nello standard.

La seconda correzione, del 2015 e relativa alla Dichiarazione di applicabilità (Statement of Applicability o SoA), è di tipo editoriale, ma con un impatto tecnico significativo. Essa chiarisce che i controlli della Dichiarazione di applicabilità non devono essere necessariamente quelli dell'Annex A della ISO/IEC 27001.

È quindi possibile usare altri elenchi di controlli, ma è comunque necessario indicare quali controlli dell'Annex A sono esclusi. Questo richiede quindi una verifica di completezza dell'elenco dei controlli rispetto all'Annex A e pertanto molti hanno comunque preferito usare direttamente l'Annex A per la propria Dichiarazione di applicabilità. Ciò non toglie che questa correzione permette di utilizzare la norma in modo più flessibile.

Le modifiche all'Appendice A della ISO/IEC 27001:2022

L'Appendice A della ISO/IEC 27001:2022 è stata modificata per allinearla alla ISO/IEC 27002:2022. I controlli di questa norma sono stati ridotti 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**: suggerisce di monitorare canali di comunicazione per ricevere informazioni sulle minacce che potrebbero compromettere le informazioni dell'organizzazione, in modo da attivare tempestivamente le necessarie misure di sicurezza; alcuni canali possono essere i bollettini dei produttori del software utilizzato, il CSIRT Italia e la Protezione civile;
- **5.23 Information security** for use of cloud services: specifica, oltre a quanto proposto dagli altri controlli relativi ai fornitori, misure di sicurezza da prevedere quando si usano fornitori di servizi cloud;
- **5.30 ICT readiness for business continuity**: richiede che venga pianificata la continuità operativa per i sistemi informatici; questo controllo si sovrappone parzialmente al 5.29 (sicurezza delle informazioni durante le interruzioni), che però è più generale e richiede anche lo sviluppo di piani di continuità operativa;
- **7.4 Physical security monitoring**: relativo agli strumenti attivi di controllo della sicurezza fisica (telecamere e allarmi);
- **8.9 Configuration management**, per la configurazione sicura di server, dispositivi e applicazioni; questo controllo include l'adozione di tecniche di hardening per i sistemi critici; esso, nella precedente versione della norma, era colpevolmente solo accennato nel controllo relativo alle procedure operative;
- **8.10 Information deletion**, relativo alla necessità di cancellare le informazioni al termine dei tempi di conservazione previsti o, nel caso in cui siano trattate per conto di un cliente, al termine del rapporto di lavoro con quel cliente; questo controllo era in precedenza accennato in quello relativo all'inventario degli asset; con la ISO/IEC 27002:2022 è stato ampliato per la sempre maggiore importanza assunta dalle tematiche di trattamento dei dati personali;
- **8.11 Data masking**, sull'anonimizzazione e pseudonimizzazione dei dati, introdotto per la sempre maggiore importanza assunta dalle tematiche di trattamento dei dati personali;
- **8.12 Data leakage prevention**, sull'uso di strumenti con funzionalità di DLP;
- **8.16 Monitoring activities**, in precedenza, incluso tra i controlli relativi al logging; ora è stato giustamente valorizzato;
- **8.23 Web filtering**, in precedenza incluso tra i controlli di rete, ora è stato meglio evidenziato;
- **8.28 Secure coding**, in precedenza incluso nel controllo relativo alla politica di sviluppo sicuro (oggi più chiaramente denominato "Ciclo di vita dello sviluppo sicuro").

Alcuni tra i controlli più estesi nella ISO/IEC 27002:2022 sono suddivisi in **sotto-controlli**. Questi non risultano presenti nell'Appendice A della ISO/IEC 27001:2022 perché essa riporta solo i controlli. Alcuni sotto-controlli però sono degni di nota perché sottolineano alcuni aspetti in precedenza non ben evidenziati. Tra questi vi sono:

- **controllo dei visitatori**, parte del controllo sugli accessi fisici;
- **trasferimenti orali delle informazioni**, parte del controllo sul trasferimento delle informazioni;

- **requisiti contrattuali** dei clienti dell'organizzazione che adotta la ISO/IEC 27001, parte del controllo "Requisiti legali, statutari, regolamentari e contrattuali", spesso affrontato solo relativamente ai requisiti legali.

Altri controlli hanno cambiato significativamente il nome, che denuncia anche alcuni cambiamenti di contenuto, tra questi:

- "**Identity management**", in precedenza "Registrazione e de-registrazione degli utenti", è stato ampliato;
- "**Information security during disruption**", in precedenza "Pianificazione della continuità della sicurezza delle informazioni", è stato ristrutturato per chiarire ulteriormente il fatto che la ISO/IEC 27001 non si occupa di continuità operativa (business continuity), ma solo della sua parte relativa alla sicurezza delle informazioni;
- "**User endpoint devices**", che amplia notevolmente il precedente controllo "Politica per i dispositivi portatili";
- "**Secure development life cycle**", per migliorare il titolo del precedente "Politica per lo sviluppo sicuro".

I requisiti per la transizione

IAF è l'organismo che controlla **gli accordi di mutuo riconoscimento** tra organismi di accreditamento membri di IAF (tra cui l'italiano Accredia), in modo che i risultati degli organismi di certificazione da essi accreditati siano accettati globalmente.

Le pubblicazioni MD (mandatory document) di IAF riportano i requisiti che gli organismi di accreditamento membri di IAF e quelli di certificazione accreditata devono rispettare. IAF ha pubblicato il documento IAF MD 26:2022 "Transition requirements for ISO/IEC 27001:2022".

I requisiti per la transizione sono stati pubblicati a giugno 2022, in largo anticipo rispetto alla pubblicazione della ISO/IEC 27001:2022, visto che questa era ormai in stato di bozza finale, diversa rispetto alla versione definitiva solo per correzioni editoriali.

La MD 26 indica che **gli organismi di certificazioni** dovranno aver concluso la transizione dei certificati ISO/IEC 27001:2013 alla ISO/IEC 27001:2022 entro 3 anni dalla pubblicazione della norma stessa. Oggi si può quindi dire che tutte le organizzazioni dovranno aver ricevuto un audit di transizione al massimo entro il 31 ottobre 2025.

Per quanto riguarda le nuove certificazioni, gli organismi di certificazione dovranno offrirle entro il 31 ottobre 2023, un anno dopo la pubblicazione della norma.

La MD 26 permette di svolgere gli audit di transizione durante un audit di sorveglianza o ri-certificazione già programmato oppure durante un audit separato.

L'audit di transizione non potrà essere documentale, ma dovrà prevedere un riesame sul campo dei controlli tecnologici nuovi o modificati scelti dall'organizzazione. Restano comunque permesse in generale le attività di audit da remoto.

Altri cambiamenti a catena (27003 & c.)

Nel 2021, il WG 1 ha definito un "phased revision plan". Secondo questo piano, tutte le norme legate alle ISO/IEC 27001 e 27002 saranno aggiornate per riflettere i

cambiamenti di queste ultime e, non potendole aggiornare tutte insieme a causa del numero purtroppo non illimitato di esperti facenti parte del WG 1, saranno divise in tre principali scaglioni dando priorità a quelle con cambiamenti più sostanziali.

Il primo scaglione di lavori è già quasi completato e include le ISO/IEC 27009, 27011 e 27017; il secondo, i cui lavori sono già avviati, le ISO/IEC 27000, 27008, 27019 e il terzo, attualmente pianificato, le ISO/IEC 27003, 27004, 27007. Questo porterà ad avere, auspicabilmente entro il 2025, un insieme coordinato di norme aggiornate ed efficacemente impiegabili in modo sinergico.

In parallelo, il WG 5, gruppo dedicato agli standard relativi alla privacy, ha iniziato i lavori sulla ISO/IEC 27701, sui sistemi di gestione per la privacy, e sulla ISO/IEC 27018, relativa ai controlli privacy per i fornitori di servizi cloud.

La futura revisione 2025

A conclusione di questo ciclo di revisione, verso fine 2023, si prevede di avviare una nuova valutazione di aggiornamento dei contenuti della ISO/IEC 27001, ritornando sulle meccaniche, dallo "statement of applicability" alla suddivisione dei requisiti applicabili ai fornitori, che il WG 1 sta al momento discutendo in modo informale con pubblicazioni dette "auditor practice notes". Esse saranno progressivamente pubblicate in modo gratuito **sul nuovo sito ad esso dedicato**.

Gli eventuali frutti di questa attività verosimilmente traguarderanno una quarta edizione della ISO/IEC 27001, al momento prevista per il 2025 ma che, come l'esperienza ci insegna, molto facilmente sarà successiva.

Conclusioni

La nuova ISO/IEC 27001 presenta numerose modifiche rispetto alla versione precedente, ma quelle veramente significative sono quelle relative ai controlli di sicurezza presenti nell'Appendice A. La gran parte di questi controlli sono in realtà miglioramenti di quelli precedenti e, pertanto, un'organizzazione con un buon livello di sicurezza non dovrebbe aver problemi ad aggiornare il proprio sistema di gestione per la sicurezza delle informazioni.

La stessa IAF scrive che l'impatto dei cambiamenti della ISO/IEC 27001:2022 è limitato all'introduzione di una nuova Appendice A, ma i requisiti della norma non richiedono di adeguare i propri controlli a esso, bensì di confrontarli con esso dopo aver scelto quelli necessari, in modo da evitare che dei controlli necessari siano stati omessi. Questo confronto non dovrebbe portare alla "scoperta" di controlli necessari e, se questo dovesse succedere, l'organizzazione dovrebbe aggiornare tempestivamente il proprio piano di trattamento del rischio e attuarli.

In conclusione, la stessa IAF stabilisce che "l'impatto della ISO/IEC 27001:2022 sulle organizzazioni che hanno attuato un sistema di gestione per la sicurezza delle informazioni non deve essere significativo" ma permetterà verosimilmente di gestire in modo sensibilmente più efficace ed anche sinergico con altri schemi i controlli relativi alla sicurezza delle informazioni.

Per questo motivo raccomandiamo la transizione alla prima verifica utile, considerando che **il lavoro più oneroso è di tipo documentale**, ossia di aggiornamento dell'attività di risk assessment e della dichiarazione di applicabilità (SOA), già comunque oggetto di riesame almeno annuale.

Decisioni più rapide con l’intelligenza artificiale