KNOSSO
Knowledge for a Safe and Secure Organization

La nuova ISO 27001

Terza edizione della ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems"

"Per affrontare le sfide globali della sicurezza informatica e migliorare la fiducia digitale, è stata pubblicata una versione nuova e migliorata di ISO/IEC 27001. Lo standard più noto al mondo sulla gestione della sicurezza delle informazioni aiuta le organizzazioni a proteggere le proprie risorse informative, vitali nel mondo sempre più digitale di oggi".

La nuova ISO 27001:2022 con gli standard su sicurezza delle informazioni, cybersecurity e privacy.

Come ampiamente atteso, a fine dello scorso anno è uscita la terza edizione **della ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection — Information security management systems — Requirements**"; si tratta della norma di riferimento sui Sistemi di gestione della sicurezza delle informazioni che prevede requisiti e controlli per garantire il rispetto dello standard. In questo articolo si desidera illustrare la struttura della nuova edizione della norma e fornire alcune indicazioni specifiche.

L'obiettivo della norma è quello di fornire alle organizzazioni gli strumenti di base per proteggere il patrimonio delle informazioni (compresi i dati personali; considerando che gli attacchi informatici sono in continua crescita, non risparmiano alcun tipo di azienda ed utilizzano tecniche sempre più sofisticate. Il rapporto annuale - Global Cybersecurity Outlook 2022 - pubblicato dal World Economic Forum indica che attacchi informatici sono aumentati del 125% rispetto all'anno precedente e la tendenza prosegue anche per il 2022.

La ISO/IEC 27001:2022 non è una norma "tecnica", ma al contrario un framework – di requisiti e controlli – da gestire centralmente, che attraversa i vari processi aziendali (e non solo quelli che impattano sull'ICT), integrabile con altri sistemi di gestione.

I princìpi che hanno guidato la nuova revisione della norma (compresi i controlli di cui di seguito si dà conto) sono orientati a garantire:

- la disponibilità, riservatezza e disponibilità dei dati;
- - un approccio dinamico (in continua evoluzione) basato su individuazione delle minacce e delle vulnerabilità;
- - la protezione delle informazioni in tutte le forme e supporti (cartacei, cloud, digitali e verbali);
- - l'aumento della resilienza agli attacchi informatici;
- - eliminazione di misure che si dimostrano inefficaci.

Le modifiche ai requisiti e controlli - La norma come noto prevede, a differenza di altre norme sui sistemi di gestione, sia un apparato di requisiti che di controlli.

Oltre alla sicurezza informatica sono inclusi anche gli aspetti legati alla gestione della privacy oltre al "control language" che è stato aggiornato.

Le modifiche ai controlli di sicurezza (Dichiarazione di Applicabilità) sono piuttosto significative diverse modifiche.

In generale:

- introdotte le nuove tecnologie digitali (Cloud e automazione) in considerazione di adozione crescente di tali tecnologie;
- evidenziati rischi per la sicurezza informatica e la privacy;
- mutevolezza della tipologia di minacce (malware e ransomware);
- considerate best practice quail NIST, COBIT, ecc.
- aggiornamento del Vontrol Language (CL).

In particolare, per requisito:

a) si richiede un'analisi di quali dei requisiti delle parti interessate devono essere affrontati attraverso il sistema di gestione per la sicurezza delle informazioni;
b) è richiesto che ci sia una pianificazione dei processi e delle loro interazioni nell'ambito del sistema di gestione;
c) viene messo in evidenza che la comunicazione dei diversi ruoli è interna all'organizzazione;
d) si fissa requisito del monitoraggio degli obiettivi;
e) si richiede la pianificazione di qualsiasi modifica al sistema di gestione diventa un requisito;
f) vengono introdotti nuovi requisiti per stabilire criteri per i processi di sicurezza e per la loro conseguente implementazione mentre non è più un requisito l'attuazione di piani per il raggiungimento degli obiettivi;
g) si specifica che in relazione agli aspetti delle parti interessate questi devono riguardare specificatamente le loro esigenze e aspettative rilevanti per il sistema di gestione per la sicurezza;
h) vengono rinumerate le clausole senza variazioni nei contenuti;

Insomma, vi sono 35 controlli invariati, 11 nuovi controlli, 23 rinominati, 57 accorpati, 1 suddiviso in 2 controlli separati: tuttavia i controlli appaiano non particolarmente variati.

In generale poi qualche variazione/modifica sull'High Level Structure (HLS) dell'ISO che si basano sull'ultima versione dell'Annex SL delle Direttive ISO/IEC Parte 1 (2022).

Il periodo di transizione è fissato in 3 anni. Pertanto – verrà predisposto uno specifico piano di transizione di dettaglio - le Organizzazioni certificate sulla base della edizione 2013 dovranno pianificare e recepire le modifiche entro i TRE anni provvedendo alla transizione del proprio Certificato di Registrazione entro e non oltre il 31 ottobre 2025 (durante una verifica di sorveglianza / rinnovo o eseguendo una verifica straordinaria).

La modifica più significativa, rispetto alla precedente versione del 2013, riguarda la dichiarazione di applicabilità così come richiesta dal capitolo 6 che non deve essere più necessariamente redatta sulla base dei controlli dell'Allegato A. Il documento può seguire un qualunque impianto di controlli purché sia compliance con quelli dell'Allegato A ed eventualmente ne aggiunga di nuovi.

Questo modello, per quanto nuovo nell'approccio, di fatto ricalca quanto anche già previsto nella precedente versione della norma che permetteva un set di controlli comunque più ampio di quello previsto dall'Allegato A. Si consiglia, qualora si decidesse di applicare questo approccio, di predisporre una tabella di correlazione tra il set di controlli applicato e quello previsto dall'Allegato A in modo da facilitare la lettura.

Non si rilevano ulteriori significative modifiche per quanto riguarda i requisiti e questo può facilitare sicuramente la transazione.

Tali modifiche erano già note da febbraio con la pubblicazione della ISO/IEC 27002:2022 "Information security, cybersecurity and privacy protection — Information security controls" (pubblicata a febbraio 2022). I controlli per altro sono la parte caratterizzante del documento: la ISO/IEC 27002:2022 fornisce le linee guida e una serie di informazioni di supporto per la corretta applicazione dei controlli previsti dallo standard.

Le modifiche introdotte anche grazie alla presenza degli 11 nuovi controlli permette di rendere i sistemi di gestione della sicurezza delle informazioni sempre più aderenti ad una tecnologia in continua evoluzione.

La modifica del titolo dello standard - La ISO/IEC 27001:2022 rispetto alla versione precedente ha anche modificato il titolo:

- da “Information technology — Security techniques — Information security management systems — Requirements”
- a ”Information security, cybersecurity and privacy protection — Information security management systems — Requirements”

L’introduzione dei concetti di cybersecurity e di protezione dei dati personali è un ulteriore elemento che rafforza quanto questo standard può essere considerata come una potente misura di accountability a supporto di quanto richiede il GDPR. Del resto, tra i controlli della norma sono stati sempre presenti alcuni dedicati esplicitamente alla protezione dei dati personali sia in modo diretto che indiretto.

Per amore di precisione tutte le norme sui sistemi di gestione per la sicurezza delle informazioni che fanno capo al Comitato tecnico ISO/IEC JTC 1/SC 27 hanno modificato la prima parte del “titolo”.

ISO/IEC 27001:2022 “Information security, cybersecurity and privacy protection — Information security management systems

Un riferimento al GDPR

La norma non soddisfa i requisiti dell’art. 42” Certificazione” del GDPR in quanto gli Organismi di certificazione che possono certificare le aziende a fronte dello standard devono essere accreditati rispetto alla EN-ISO/IEC 17065/2012 come richiesto dall’art 43, come ad esempio avviene con altri standard come quello di Europrivacy, approvato di recente dall’European Data Protection Board.

La ISO/IEC 27001:2022 resta comunque un caposaldo per quanto riguarda sicurezza delle informazioni e non dare la giusta valenza significa non dare valore all’insieme dei requisiti e dei controlli che questa norma porta in dote per proteggere tutte le parti interessate.

I tempi di transizione dei certificati ISO/IEC 27001:2013 - Le aziende certificate a fronte della ISO/IEC 27001:2013 hanno tempo fino al 31 ottobre 2025 per effettuare la transizione. Dato che le modifiche sono di lieve entità e quelle più rilevanti sui controlli sono già note da febbraio 2022 la transizione non è complessa.

Quindi, anche in questo caso sono forniti tre anni “canonici” di tempo per permettere ad ogni organizzazione di effettuare il passaggio. Si resta comunque in attesa di indicazioni puntuali da parte di Accredia.

Per le organizzazioni che stanno affrontando l’implementazione della nuova norma si raccomanda di utilizzare la nuova versione dello standard.

La famiglia delle norme ISO/IEC 27000 è in continua evoluzione, nella stessa data in cui è stata pubblicata la ISO/IEC 27001:2022 è stata anche pubblicata la ISO/IEC 27005:2022 “Information security, cybersecurity and privacy protection — Guidance on managing information security risks”. Altre linee guida della medesima famiglia sono in corso di pubblicazione e revisione.

A valle dell’aggiornamento della ISO/IEC 27001:2022 è previsto come indicato nel sito della ISO, anche l’aggiornamento della ISO/IEC 27701:2019 “Security techniques — Extension to ISO/IEC 27001 and ISO/IEC

27002 for privacy information management — Requirements and guideline" – alla data della redazione dell'articolo è stata conclusa la fase di "Committee" ed è in fase di avvio quella di "Enquiry".

Insomma, la norma aggiornata nuova specifica i requisiti per stabilire, implementare, mantenere e migliorare continuamente un sistema di gestione della sicurezza delle informazioni nel contesto dell'organizzazione. Include anche i requisiti per la valutazione e il trattamento dei rischi per la sicurezza delle informazioni adattati alle esigenze dell'organizzazione. I requisiti stabiliti nel documento sono generici e si intendono applicabili a tutte le organizzazioni, indipendentemente dal tipo, dimensione o natura.

Ormai è noto quasi a tutti che la criminalità informatica sta diventando sempre più grave e sofisticata poiché gli hacker sviluppano tecniche di criminalità informatica più avanzate. Il rapporto Global Cybersecurity Outlook del World Economic Forum indica che gli attacchi informatici sono aumentati del 125% a livello globale nel 2021, con prove che suggeriscono un continuo aumento fino al 2022. In questo panorama in rapida evoluzione, i leader devono adottare un approccio strategico ai rischi informatici.

L'obiettivo della norma è quello di fornire alle organizzazioni gli strumenti di base per proteggere il patrimonio delle informazioni, compresi i dati personali. La ISO/IEC 27001:2022 non è una norma "tecnica", ma al contrario un framework – di requisiti e controlli – da gestire centralmente, che attraversa i vari processi aziendali (e non solo quelli che impattano sull'ICT), integrabile con altri sistemi di gestione.

I princìpi che hanno guidato la nuova revisione della norma sono orientati a garantire:

- la disponibilità, riservatezza e disponibilità dei dati;
- un approccio dinamico (in continua evoluzione) basato su individuazione delle minacce e delle vulnerabilità;
- la protezione delle informazioni in tutte le forme e supporti (cartacei, cloud, digitali e verbali);
- l'aumento della resilienza agli attacchi informatici;
- eliminazione di misure che si dimostrano inefficaci.

Tali modifiche erano già note da febbraio 2022 con la pubblicazione della ISO/IEC 27002:2022 "Information security, cybersecurity and privacy protection — Information security controls" I controlli per altro sono la parte caratterizzante del documento: la ISO/IEC 27002:2022 fornisce le linee guida e una serie di informazioni di supporto per la corretta applicazione dei controlli previsti dallo standard.

Le modifiche introdotte anche grazie alla presenza degli undici nuovi controlli permette di rendere i sistemi di gestione della sicurezza delle informazioni sempre più aderenti ad una tecnologia in continua evoluzione.

Nel mezzo della quarta rivoluzione industriale, l'interdipendenza sistemica crea sia costi al ribasso del rischio informatico che un valore al rialzo molto maggiore", afferma Andreas Wolf, che guida il gruppo di esperti responsabili dello standard. "Le organizzazioni che ci condurranno nel futuro digitale sono quelle che non solo sono abbastanza vulnerabili da ammettere che non possono farcela da sole, ma sono anche abbastanza sicure ed esperte da rendersi conto che è meglio che le aziende non ci provino".

Le organizzazioni che adottano la resilienza informatica attraverso una vulnerabilità sicura emergono rapidamente come leader nel loro settore e stabiliscono lo standard per il loro ecosistema. L'approccio olistico di ISO/IEC 27001 significa che l'intera organizzazione è coperta, non solo l'IT. Persone, tecnologia e processi ne traggono vantaggio.

Lo standard “principe” per la sicurezza delle informazioni ha subito rilevanti modifiche per la componente dei controlli, come già noto da diversi mesi. L’aggiornamento della norma, a cui ne seguiranno altre che su questa si appoggia, è l’occasione per rivedere e migliorare lo stato delle misure poste in atto a tutela della sicurezza delle informazioni, nell’ambito delle quali sono comprese anche quelle a protezione dei dati personali. Nello specifico:

- protegge le informazioni in tutte le forme, compresi i dati cartacei, cloud e digitali;
- aumenta la resilienza agli attacchi informatici;
- fornisce un framework gestito centralmente che protegge tutte le informazioni in un’unica posizione;
- garantisce la protezione a livello di organizzazione, anche contro i rischi basati sulla tecnologia e altre minacce;
- risponde alle minacce alla sicurezza in evoluzione;
- riduce i costi e la spesa per tecnologie di difesa inefficaci;
- protegge l’integrità, la riservatezza e la disponibilità dei dati.

Le Organizzazioni che adottano la resilienza informatica emergono rapidamente come leader nel loro settore e stabiliscono lo standard per il loro ecosistema. L’approccio olistico di ISO/IEC 27001 significa che l’intera organizzazione è coperta, non solo l’IT. Persone, tecnologia e processi ne possono trarre vantaggio e dimostra agli stakeholder, ai partners e ai clienti, l’impegno dell’organizzazione a gestire le informazioni in modo sicuro.

Fonti: Insic; CertiW; Federprivacy; Cybersecurity360; Accredia; ISOCertificazioni; “5G e cyber security. Tutte le ragioni di una sfida cruciale” B. Costanzo