La norma ISO 27002:2007

Caratteristiche

La Norma **è stata redatta** e pubblicata nell'ottobre 2005 (la versione italiana UNI è del 2006) a fini certificativi, **in modo da costituire un sistema completo per garantire la gestione della sicurezza nella tecnologia dell'informazione**: con la sua pubblicazione ha sostituito la norma inglese BS 7799:2 (che conteneva la linea guida e lo standard vero e proprio), che fino ad allora rappresentava la principale norma di riferimento per l'applicazione di un Sistema di Gestione per la sicurezza delle informazioni. Il nuovo standard ha assorbito entrambe le parti: la linea guida è stata recepita dall'ISO come ISO 17799 (Information Technology -Security Techniques - Code of practice for information security management), mentre la seconda parte, lo standard vero e proprio, è stato emesso nell'ottobre 2005 come ISO 27001. Nel 2007 anche il documento ISO 17799 è stato ritirato e sostituito dalla norma ISO 27002, meglio coordinata con la ISO 27001 e parte della serie 27000 che comprende oggi svariati altri documenti correlati al tema della sicurezza delle informazioni.

La norma ISO 27002:2007 è una raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001:2005 al fine di proteggere le risorse informative; ISO 27001:2005 è il documento normativo di certificazione al quale l'organizzazione deve fare riferimento per costruire un Sistema di Gestione della Sicurezza delle Informazioni che possa essere certificato da un ente indipendente, mentre la norma ISO 27002:2007 non è certificabile in quanto è una semplice raccolta di raccomandazioni.

Dal momento che l'informazione è un bene che aggiunge valore all'impresa, e che ormai la maggior parte delle informazioni sono custodite su supporti informatici, ogni organizzazione deve essere in grado di garantire la sicurezza dei propri dati, in un contesto dove i rischi informatici causati dalle violazioni dei sistemi di sicurezza sono in continuo aumento. L'obiettivo del nuovo standard ISO 27001:2005 è proprio quello di proteggere i dati e le informazioni da minacce di ogni tipo, al fine di assicurarne l'integrità, la riservatezza e la disponibilità, e fornire i requisiti per adottare un adeguato sistema di gestione della sicurezza delle informazioni (SGSI) finalizzato ad una corretta gestione dei dati sensibili dell'azienda.

La norma è applicabile a imprese operanti nella gran parte dei settori commerciali e industriali, come finanza e assicurazioni, telecomunicazioni, servizi, trasporti, settori governativi.

L'impostazione dello standard ISO/IEC 27001 è coerente con quella del Sistema di Gestione per la Qualità ISO 9001:2015 ed il Risk management, basandosi sull'approccio per processi, strutturato in politica per la sicurezza, identificazione, analisi dei rischi, valutazione e trattamento dei rischi, riesame e rivalutazione dei rischi, modello PDCA, utilizzo di procedure e di strumenti come audit interni, non conformità, azioni correttive e preventive, sorveglianza, nell'ottica del miglioramento continuo.

La norma Standard ISO 27001:2005 stabilisce i requisiti per il Sistema di Gestione della Sicurezza delle Informazioni (ISMS). L'obiettivo principale è quello di stabilire un sistema per la gestione del rischio e la protezione delle informazioni e degli asset ICT. La norma è applicabile a tutte le imprese private o pubbliche, in quanto prescinde da uno specifico settore di business o dall'organizzazione dell'azienda. Però bisogna tener presente che l'adozione e gestione di un ISMS richiede un impegno di risorse significativo e quindi deve essere seguito da un ufficio specifico, il quale in genere coincide con l'ufficio Organizzazione e Qualità.

> “Essa specifica i requisiti per impostare, mettere in opera, utilizzare, monitorare, rivedere, manutenere e migliorare un sistema documentato all'interno di un contesto di rischi legati alle attività centrali dell'organizzazione. Dettaglia inoltre i requisiti per i controlli di sicurezza personalizzati in base alle necessità di una singola organizzazione o di una sua parte. Il sistema è progettato per garantire la selezione di controlli di sicurezza adeguati e proporzionati.”

Lo standard ISO 27001:2005 che come già detto presenta molti punti in comune con la ISO 9001, che definisce i requisiti di un sistema di gestione della qualità (es. adozione modello PDCA, filosofia del miglioramento continuo, ecc.), si differenzia in quanto segue un approccio basato sulla gestione del rischio. Quindi lo standard prevede:

- Pianificazione e Progettazione;
- Implementazione;
- Monitoraggio;
- Mantenimento e Miglioramento

similmente a quanto previsto dai sistemi per la gestione della qualità.

Nella fase di progettazione richiede però lo svolgimento di un risk assessment, schematizzabile in:

- Identificazione dei rischi;
- Analisi e valutazione;
- Selezione degli obiettivi di controllo e attività di controllo per la gestione dei rischi;
- Assunzione del rischio residuo da parte del management;
- Definizione dello Statement of Applicability.

L'ultimo punto specifica gli obiettivi di controllo adottati e i controlli implementati dall'organizzazione rispetto ad una lista di obiettivi di controllo previsti dalla norma. Analogamente alla norma sui sistemi di qualità, il sistema deve essere documentato, ma in aggiunta è richiesta ampia documentazione riguardo sia l'analisi del rischio sia le procedure e i controlli a supporto dell'ISMS. Come per il sistema qualità, l'organizzazione ISMS può essere certificata da enti di certificazione, che operano tramite valutatori qualificati, esaminando periodicamente lo stato delle condizioni di conformità. Tra le condizioni di conformità la norma prevede la pianificazione e realizzazione di attività di autocontrollo gestite dall'impresa, con personale proprio o esterno, purché in entrambi i casi dotato delle necessarie competenze.

Controlli

Di fondamentale importanza è l'Annex A "Control objectives and controls" che contiene i 133 "controlli" a cui l'organizzazione che intende applicare la norma deve attenersi.

Essi vanno dalla politica e l'organizzazione per la sicurezza alla *gestione dei beni* e alla *sicurezza delle risorse umane*, dalla sicurezza *fisica e ambientale* alla gestione delle *comunicazioni* e dell'*operativo*, dal controllo degli accessi *fisici* e *logici* alla gestione di un monitoraggio e trattamento degli incidenti (relativi alla sicurezza delle informazioni).

La gestione della Business Continuity e il *rispetto normativo*, completano l'elenco degli *obiettivi di controllo*.

L'organizzazione deve motivare quali di questi controlli non sono applicabili all'interno del suo ISMS, per esempio un'organizzazione che non attua al suo interno 'commercio elettronico' può dichiarare non applicabili i controlli 1-2-3 del A.10.9 che si riferiscono appunto all'e-commerce.

Privacy-Safety

La conformità alla ISO 27001, pur certificata da un organismo di certificazione, magari accreditato, non solleva l'organizzazione dal rispetto delle misure minime di sicurezza e dalla produzione della documentazione richiesta dalla legge sulla Privacy; il controllo A.18.1.4 richiede infatti che "La protezione dei dati e della privacy deve essere garantita come richiesto nella legislazione, nelle norme e, se applicabile, nelle clausole contrattuali".

La differenza sostanziale tra legge sulla Privacy e la norma ISO 27001 è che la legge sulla privacy tutela dati personali, sensibili e non, mentre la ISO 27001 pur richiedendo che ciò sia fatto, s'interessa anche dei dati di *business* dell'organizzazione che devono essere salvaguardati per l'interesse stesso dell'organizzazione.

Il D.Lgs.81/2008, che in Italia regolamenta la sicurezza sui luoghi di lavoro, viene in genere individuato tra quelle normative la cui osservanza deve essere esplicitamente definita e documentata, come previsto nel controllo A.18.1.1 che parla appunto della legislazione *applicabile*.

Il soddisfacimento dei requisiti di legge non è condizione sufficiente al test della ISO 27001. Per esempio un *impianto antincendio* posto a salvaguardia di un ambiente in cui sono installati dei server o dei client, che contengono informazioni incluse nel dominio di certificazione che soddisfi i requisiti di legge, non soddisfa automaticamente le esigenze che esprime la norma ISO 27001, che si preoccupa anche della 'correttezza' dei 'dati' contenuti nei server e nei client, cosa non automaticamente garantita da un sistema antincendio conforme alle legge dello stato.