La norma ISO/IEC 27001:2013, una chiave di lettura semplice

Date : 26 aprile 2018

26Prima perché e poi come

Mi capita sempre più spesso di ricevere richieste di attività in ambito ISO 27001; è evidente che il livello di attenzione ai temi di sicurezza delle informazioni è cresciuto e come conseguenza, per fronteggiare tale necessità, ci si riferisce allo standard più consolidato e "conosciuto". Tuttavia, altrettanto spesso, l'approccio è un po' confuso: "*Voglio la certificazione ISO 27001 dei sistemi IT aziendali"* o *"Voglio certificare il mio prodotto*" sono richieste che hanno avuto una certa ricorrenza ed, in alcuni casi, a nulla è valso un tentativo di ragionamento sul corretto focus. Per tale motivo l'argomento che intendo affrontare è il seguente: la norma ISO/IEC 27001:2013 non è uno standard di sicurezza informatica ma di sicurezza delle informazioni; applicando i requisiti si può certificare il sistema di gestione per la sicurezza delle informazioni e null'altro.

Con questo articolo e con quelli che verranno, vorrei fare chiarezza sul tema, svincolandomi per quanto possibile dagli aspetti tecnici dello standard e dandone una chiave di lettura semplice e pratica. Voglio precisare sin da ora che *la chiave di lettura semplice* non corrisponde alla semplicità di applicazione dello standard, che rimane un percorso impegnativo a tutti i livelli ma di significativa crescita.

Il quadro dell'organizzazione

Se consideriamo un'azienda, indipendentemente dalle dimensioni e dalla complessità, essa è un insieme organizzato di entità, finalizzate a raggiungere degli obiettivi. Per raggiungere tali obiettivi ogni entità deve dare il proprio supporto, per questo c'è bisogno del marketing, dell'IT, del commerciale, degli acquisti, etc. In questo contesto vanno ad inserirsi i sistemi di gestione per la sicurezza delle informazioni come elemento essenziale per supportare le attività di business e proteggere le informazioni, in ogni formato.

L'informazione, se gestita opportunamente, è in grado di suggellare il successo od il fallimento di un progetto; per quanto sembrino inflazionate, la riservatezza, la disponibilità e l'integrità sono le principali proprietà dell'informazione, a cui dobbiamo fare riferimento e di cui è

fondamentale conoscerne il valore. Lo standard entra nel merito di queste tematiche incentivando l'information security governance come elemento a supporto del business.

Cosa è, prima conoscere e poi operare

La norma definisce i requisiti da applicare per la realizzazione ed il miglioramento continuo (Deming cycle, nda) di un sistema di gestione per la sicurezza delle informazioni (SGSI). In altre parole definisce un framework strutturato e basato sul rischio, per proteggere il proprio patrimonio informativo.

"Basato sul rischio", sembra un'accezione fatalista ma la nostra vita ruota da sempre intorno a questo concetto: prima di attraversare la strada, non siamo forse abituati a guardare a sinistra ed a destra? Qualunque attività svolgiamo nel quotidiano ha in sé dei rischi che valutiamo e gestiamo continuamente, quasi senza rendercene conto. Se invece vediamo il rischio nell'accezione positiva, possiamo trovare delle opportunità, che se seguite potrebbero migliorare significativamente il contesto in cui operiamo. Lo stesso principio si applica alla protezione delle informazioni, ma prima di agire o comunque con periodicità. La ISO/IEC 27001:2013 si basa su questo principio, declinato ad un livello più alto dalla ISO 31000:2018 (*Risk Management*) ed a un livello più di dettaglio dalla ISO/IEC 27005:2011 (*Information Security Risk Management*, in revisione). Tuttavia, culturalmente si fa una certa fatica a percepire tali tipologie di rischio ma quanto accade quasi quotidianamente nelle nostre immediate vicinanze sta lentamente invertendo tale polarità.

No IT, la tecnologia è un di cui

No IT, non è lo scenario di un piano di continuità operativa ma un altro punto oscuro su cui è bene fare chiarezza**: la ISO/IEC 27001:2013 non è una norma IT!** Forse qualcuno sarà inorridito da tale asserzione ma se ne leggiamo il corpo non vi troviamo nulla che può essere ricondotto direttamente all'information technology. È altrettanto vero però che l'IT svolge un ruolo importante per la protezione delle informazioni, tuttavia non è l'elemento centrale.

Da una lettura superficiale, ma col cervello acceso, la norma ci dice di capire chi siamo, dove ci muoviamo e chi sono le nostre interfacce (4. Contesto e parti interessate) e di correlare tali informazioni per identificare l'ambito aziendale su cui realizzare il Sistema di Gestione ed iniziare a profilare potenziali fonti di rischio. Immediatamente dopo (5. Leadership) è recitato l'aspetto principale da tenere in considerazione: la correlazione con il business aziendale. E' in questa fase che il SGSI assume con maggiore risalto il ruolo di supporto della Direzione. Viene chiesto infatti di declinare degli obiettivi di sicurezza delle informazioni ad un livello più alto e di formalizzarli in una policy di sicurezza da comunicare all'interno, il primo mattoncino. Tali obiettivi non sono casuali ma identificati dalla direzione, quindi da chi ha una visione d'insieme ampia, completa e strettamente legata alle esigenze di business. È qui che ci avviciniamo al nucleo: definire gli obiettivi di sicurezza e correlarli a quelli globali dell'organizzazione. Nel passaggio successivo (6. Pianificazione) viene richiesto di riprendere gli obiettivi inseriti nella policy e declinarli in obiettivi misurabili. È sul raggiungimento di questi obiettivi che dobbiamo prima identificare le modalità di valutazione e trattamento dei rischi e delle opportunità e poi

eseguire tali attività sul campo (8. Attività operative). E questo è proprio il nucleo dello standard. Il resto dei requisiti vanno a completare il quadro di gestione della sicurezza sia per attività di supporto (7. Supporto), necessarie per mettere in campo personale con il giusto livello di consapevolezza, conoscenza ed esperienza, sia per quelle di valutazione e miglioramento. Gli audit interni (che devono essere un'analisi approfondita dei processi e non solo una formalità) e la misura delle performances infatti, vanno a completare il ciclo di Deming ed a chiudere la partita con la direzione che prima mette a disposizione le risorse necessarie e poi verifica se queste hanno portato i risultati attesi (9. Valutazione delle prestazioni). In chiusura, facciamo due considerazioni: la prima, è che qualsiasi azienda è un'entità dinamica, la seconda, è che si può sbagliare. Il check delle attività di sicurezza è finalizzato ad aggiustare il tiro (act) laddove si verifichino novità o modifiche di una certa rilevanza o situazioni difformi dalle strategie di sicurezza implementate (10. Miglioramento).

Non sono stati citati volutamente tutti i requisiti normativi per dare maggiore risalto alla filiera centrale di gestione della sicurezza delle informazioni. Come del resto non è stato volutamente citato l'allegato A, croce e delizia, che tratteremo nel prossimo articolo. Per ora teniamo a mente solo il concetto di "controlli per trattare i rischi".

SGSI, il significato sta tutto nella definizione

Per chiudere citiamo un passaggio della definizione di Sistema di Gestione: "…quella parte del sistema **complessivo** di gestione…". La parola *complessivo* racchiude un ulteriore chiave di lettura dello standard e cioè che il SGSI deve vivere insieme alle altre attività di gestione dell'azienda ed integrarsi nelle attività quotidiane di tutto il personale interno ed esterno. Sarà la sensibilità e la cultura degli attori coinvolti, a tutti i livelli aziendali, a fare da discriminante tra trarre effettivamente benefici dal SGSI e sfruttare il certificato sul mercato o per partecipare a qualche gara d'appalto. La scelta è in mano a voi.

A cura di: **Salvatore D'Emilio**