

Al via le nuove regole del professionista della security

di Gennaro Bacile di Castiglione e Massimo Marrocco

articoli

Dopo circa 12 anni dalla pubblicazione della prima versione della norma UNI 10459 che definiva i requisiti relativi all'attività professionale coinvolta nel processo di *security*, è stata pubblicata la terza versione nel giugno 2017.

L'importanza di questa norma e la necessità dei suoi aggiornamenti deriva da un lato dal continuo cambiamento evolutivo della società che pone la *security* sempre più prioritaria nella scala dei bisogni quotidiani e dall'altro dall'essere stata introdotta come riferimento nel DM 269/2010 per la regolamentazione degli istituti di vigilanza privata di maggiori dimensioni, in particolare per i requisiti di professionalità necessari per il rilascio o mantenimento della licenza.

La crescente attenzione alla sicurezza ha portato anche ad approfondire sempre più le molteplici tipologie che ne costituiscono le variegate applicazioni, così oggi la sicurezza è fondamentale, per esempio, sul lavoro, sulla tutela del patrimonio tangibile e intangibile, sulla riservatezza delle informazioni, sulla tutela ambientale, sulla continuità operativa, sulla tutela da eventi naturali o atti terroristici.

In conseguenza di ciò le conoscenze e competenze che deve possedere un professionista della *security* devono essere diversificate ma comunque il più possibile esaustive rispetto a tutte le discipline della sicurezza attualmente declinate, unendo il tutto ad abilità personali specifiche.

Queste diverse discipline hanno tutte in comune di ricondursi al trattamento e gestione del rischio per il quale esiste già una norma di riferimento mondiale UNI ISO 31000. La capacità di operare come professionista della *security* con una metodologia riferita a tale *best practice* costituisce oggi, dopo l'emanazione della norma UNI 10459 e come da questa stessa enunciato, requisito fondamentale per accedere alla certificazione professionale.

D'altra parte anche la nuova *High Level Structure* (HLS), la struttura delle norme ISO sui sistemi di gestione (SG), ormai nota a tutti coloro che operano con riferimento alle *best practices*, ha tra le novità più significative l'introduzione dell'approccio basato sul rischio, in massima parte derivato proprio dalla citata UNI ISO 31000. Pur non essendo ancora andato in porto il tentativo di sviluppare la norma sui SG per la *security* i principi che sono alla base della HLS e della UNI ISO 31000 dovrebbero essere tenuti ben presenti dal professionista della *security*, nella sua preparazione e nello svolgimento dei suoi compiti. La figura 1 è ispirata a quelle presenti nelle UNI EN ISO 14001:2015 "Sistemi di gestione ambientale - Requisiti e guida per l'uso" e UNI ISO 45001:2018 "Sistemi di gestione per la salute e sicurezza sul lavoro - Requisiti e guida per l'uso", con cenni ripresi anche da UNI EN ISO 9001:2015 "Sistemi di gestione per la qualità - Requisiti". La conoscenza dei sistemi di gestione per qualità, ambiente, salute e sicurezza sul lavoro, sicurezza delle informazioni, sicurezza della catena di fornitura (*supply chain*), continuità operativa, è tra le conoscenze richieste a un professionista della *security*, almeno a livello di conoscenza base¹.

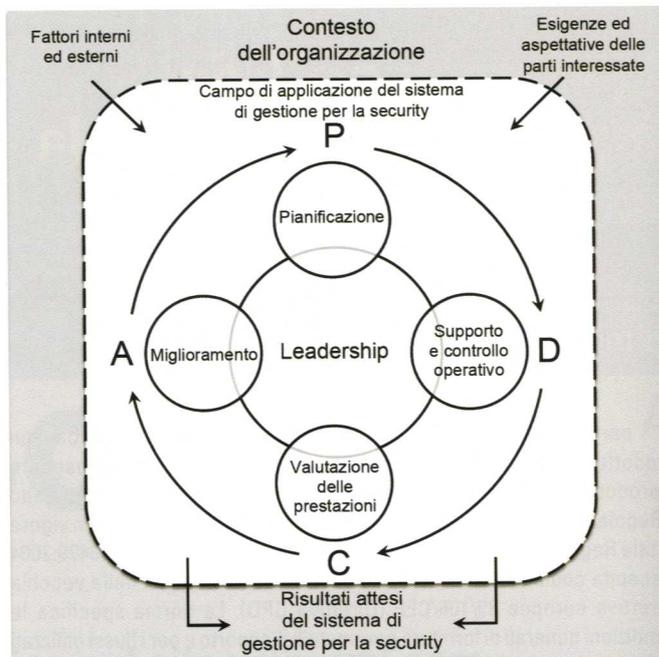


Figura 1 - Quadro di riferimento di un ipotetico sistema di gestione per la security e il ciclo PDCA.

La figura 1 illustra come un tale quadro di riferimento potrebbe essere integrato all'interno di un modello PDCA, in grado di aiutare l'alta direzione, i professionisti della security e i loro collaboratori a comprendere l'importanza di un approccio ai sistemi. Il modello può essere applicato a qualsiasi sistema di gestione e a ciascuno dei suoi singoli processi.

Può essere brevemente descritto nel modo seguente:

Plan: (Pianificare) stabilire gli obiettivi per la security e i processi necessari per fornire risultati conformi alla politica per la security dell'organizzazione.

Do: (Fare) fornire il supporto, incluse tutte le risorse necessarie e attuare i processi come pianificati.

Check: (Verificare) monitorare e misurare i processi a fronte della politica per la security, compresi i suoi impegni, degli obiettivi per la security e dei criteri operativi, e riferire i risultati.

Act: (Agire) intraprendere azioni per migliorare in continuo le prestazioni, per quanto necessario.

L'alta direzione dell'organizzazione, oltre a fissare i criteri di accettabilità dei rischi correlati alla security, dovrebbe dimostrare leadership e impegno nei riguardi di un sistema di gestione per la security mettendo a disposizione le risorse necessarie al suo funzionamento per supportare il professionista della security nello svolgimento dei suoi compiti e fornendogli sostegno per dimostrare leadership, come essa si applica alla sua area di responsabilità.

La norma UNI 10459 prevede tre diversi livelli in ordine crescente di qualificazione: *Security Expert*, *Security Manager* o *Senior Security Manager* profilati in coerenza con il Quadro Europeo delle Qualifiche (European Qualification Framework - EQF) rispettivamente ai livelli EQF 5, EQF 6 ed EQF 7. Tali livelli si riferiscono alla competenza, definita come "comprovata capacità di utilizzare conoscenze, abilità e comportamenti personali in situazioni di lavoro o di studio e nello sviluppo professionale e personale, esercitabile con un determinato grado di autonomia e responsabilità". Sostanzialmente il livello EQF 5 corrisponde alla capacità di saper gestire e sorvegliare attività nel contesto di attività lavorative esposte a cambiamenti imprevedibili, oltre a essere in grado di esaminare e sviluppare le prestazioni proprie e di altri. Il livello EQF 6 indica la capacità di saper gestire attività o progetti tecnico/professionali complessi assumendo la responsabilità di decisioni in contesti di lavoro imprevedibili, oltre a gestire lo sviluppo professionale di persone e gruppi. Il livello EQF 7 richiama la capacità di gestire e trasformare contesti di lavoro complessi, imprevedibili che richiedono nuovi approcci strategici, assumendosi la piena responsabilità delle decisioni relative, di verificare le prestazioni strategiche dei gruppi, contribuendo inoltre alla conoscenza e al miglioramento delle prassi professionali.

Note

¹ Per conoscenza base si può intendere che per la materia in oggetto una persona sia in grado di comprenderne i concetti fondamentali, avere coscienza di quando tale materia rientra nelle necessità dell'organizzazione, avere consapevolezza dei propri limiti sulla materia, ma sapere, quando se ne presentasse la necessità, dove e come approfondirne i temi di interesse e come reperire, all'interno o all'esterno dell'organizzazione per cui opera, gli esperti necessari ad affrontarne i temi specifici, per essere supportato in modo efficace ed efficiente nella soluzione dei problemi relativi.



Figura 1



Figura 2

Figura 1 - Gennaro Bacile

Figura 2 - Massimo Marrocco

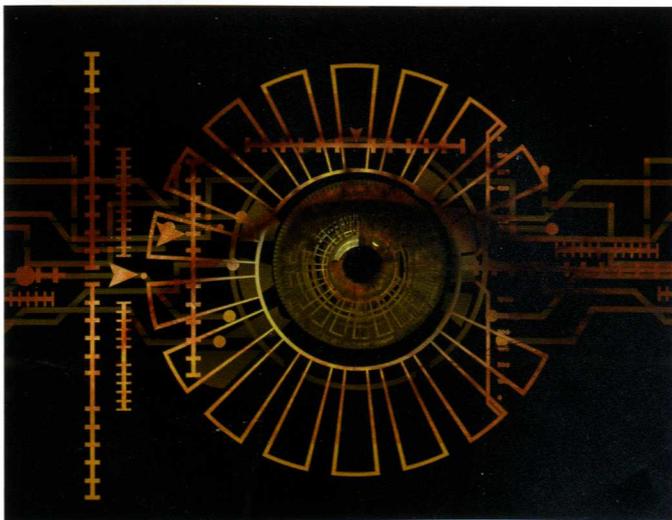
In linea generale i compiti principali di un professionista della *security* sono l'analisi del contesto di riferimento, la valutazione dei rischi (fase a sua volta formata da identificazione di tutti i rischi esogeni ed endogeni, loro analisi e misurazione) per finire con l'implementazione di un piano di trattamento degli stessi mediante l'adozione di misure di riduzione dei rischi in un'ottica di effettiva efficacia nel contenimento del danno.

Il professionista della *security* deve essere consapevole degli impatti e delle conseguenze che un rischio correlato a minacce di *security* potrebbe portare, anche indirettamente, a tutti gli aspetti significativi della vita e della sopravvivenza di un'organizzazione (immagine, reputazione, continuità operativa, costi per controversie, conformità legislativa, permessi per nuove installazioni o nuove attività, concorrenza, ecc.).

Tra le abilità e gli aspetti comportamentali di un professionista della *security* sono richieste *leadership*, capacità di incoraggiare e gestire il lavoro di gruppo, spirito di iniziativa e interesse verso le innovazioni: una caratteristica peculiare che renderebbe il professionista della *security* un elemento particolarmente prezioso per un'organizzazione è la capacità di pensare fuori dagli schemi, aver sviluppato il "pensiero laterale"².

Per esempio l'analisi di un cosiddetto "near miss" o "quasi incidente" non dovrebbe evidenziare soltanto le cause profonde dell'evento che avrebbe potuto procurare danni rilevanti, ma cercare di comprendere a fondo il perché in quel particolare evento non ci sia stato il danno che avrebbe potuto esserci. Lo scopo è quello di valutare se e in che misura tali fattori "positivi" possano o debbano divenire elementi del sistema per la protezione dai danni e comunque trarne spunto per modificare il contesto, al fine di evitare il ripetersi di un evento simile indesiderato.

Possiamo ancora dire che il professionista della *security*, per esempio, non basterà che implementi un piano di collocamento di estintori conforme alle specifiche della prevenzione incendi ma dovrà anche fornire alla committenza indicazioni per la realizzazione di un sistema di gestione che assicuri l'efficienza degli stessi, la presenza di personale addestrato all'utilizzo, il coordinamento con il Corpo dei Vigili del Fuoco in caso di *escalation*, ecc.



L'ultimo esempio citato può essere utile per chiarire la differenza concettuale tra professionista che opera nella sicurezza (esperto di prevenzione incendi) e professionista della *security* che conosce e applica le norme specifiche della prevenzione incendi ma completa la sua professione con tutte le altre discipline necessarie per assicurare l'efficacia del risultato atteso (sistemi di gestione, sicurezza dei lavoratori, sicurezza ambientale, ecc.)

Il patrimonio di conoscenze e competenze dei professionisti che operano nella *security* e quindi la normazione dei requisiti è alla base per il successivo percorso di certificazione professionale che ha come obiettivo la tutela degli interessi dei fruitori dei servizi del professionista della *security*.

Occorre chiarire che la norma non è destinata solamente al mondo della vigilanza privata ma intende profilare tutti i professionisti che operano nella sicurezza a livello di "macro visione" rispetto a tutti gli svariati ambiti specialistici. È stato il Ministero degli Interni che ha ritenuto poi di inserire i requisiti definiti dalla norma come indispensabili per il mondo della vigilanza privata, con il DM 269/2010, in un'ottica che è auspicabile sia adottata anche da altri ministeri.

La terza versione della norma UNI 10459 è stata elaborata nel 2017 sul principio del continuo miglioramento nell'obiettivo di perfezionare l'oggettività dei criteri di qualificazione dei professionisti e costituire quindi un riferimento ottimale per coloro che vogliono avvalersi dell'attività di professionisti della *security*. In particolare le varianti rispetto alla precedente versione del 2015 sono in sintesi le seguenti:

- 1) modificate alcune definizioni per rendere il significato interpretabile in maniera univoca e oggettiva;
- 2) spostato al punto 4 il paragrafo riguardante il mantenimento, l'aggiornamento e l'evoluzione delle competenze;
- 3) modificata la valutazione e convalida dei risultati dell'apprendimento, anche in questo caso per rendere il significato interpretabile in maniera univoca;
- 4) eliminato il punto 7 - Validazione dell'apprendimento;
- 5) aggiunta di un paragrafo per tener conto dei professionisti specializzati nell'ambito della sicurezza delle informazioni;
- 6) apportate altre modifiche per migliorare l'interpretazione del contenuto o per eliminare refusi.

Le varianti andranno a incidere sui percorsi sia di qualificazione sia di certificazione andando a sanare alcune divergenze interpretative, con il risultato atteso di uniformare presso tutti gli enti riconosciuti il rilascio delle qualificazioni e certificazioni secondo la norma UNI 10459:2017.

Gennaro Bacile di Castiglione

Coordinatore UNI/CT 043/GL 2 "Gestione del rischio"

Consulente, Referente Registro AICQ SICEV dei Professionisti UNI 10459

Massimo Marrocco

Coordinatore UNI/CT 043/GL5 "Organizzazione e gestione della sicurezza"

Presidente di AIPROS - Associazione Italiana Professionisti della Sicurezza

Note

² Edward de Bono: Il pensiero laterale - BUR (ISBN 88-17-13402-3) - Titolo originale: The Use of Lateral Thinking.

NEW RULES FOR THE SECURITY PROFESSIONAL

The standard UNI 10459 specifies the requirements for the professional activity in the field of security, i.e. the person with adequate competence to thoroughly manage the security process, aiming to address, with integrated global vision, the risks arising from threats of wrongful acts that could lead to loss, emergency or crisis.

The third issue of the standard has been developed in 2017 in order to continual improve objectivity of criteria for qualification of professionals in the field of security. It constitutes an optimal reference for organizations that need the services of a security manager.

You can find more details in this article.