Security Management: progettare la sicurezza in azienda

Sicurezza fisica dell'infrastruttura, sicurezza informatica, sicurezza sul lavoro, fedeltà dei dipendenti, controllo preventivo dei fornitori, applicazione del codice della privacy, anticrimine e tutela ambientale: sono solo alcuni degli ambiti di cui si occupa il Security Manager.

di Vincenzo Circosta

Definita dall'**Istat** come una delle *"12 dimensioni del benessere"* insieme alla salute, l'istruzione e il lavoro, la sicurezza è un argomento frequentemente trattato in maniera superficiale, poco approfondito e spesso preso in considerazione solo nel momento del bisogno. In azienda, la sicurezza viene gestita attraverso il **Security Management**, termine con cui si indicano

tutte quelle attività gestionali di individuazione, valorizzazione e analisi di un rischio che può provocare in un'azienda, ente o raggruppamento di beni e persone, danni patrimoniali e non (furti, frodi, divulgazione di informazioni ecc.). La persona che si occupa di tale lavoro è il responsabile della sicurezza, chiamato in inglese *"Security Manager"*.

Un riferimento per l'azienda

Il Security Manager è la figura di riferimento per l'organizzazione, la gestione e l'assunzione di responsabilità della sicurezza all'interno di un'azienda. Nel rispetto della dottrina della scienza della sicurezza il Security Manager deve essere in grado di presidiare rischi e minacce a tutto campo in relazione agli scenari sempre in evoluzione in ambito tecnico, economico, informatico, economico, finanziario, in un contesto sempre più globalizzato e interconnesso. La sicurezza aziendale ha subito infatti una profonda trasformazione, che ha modificato gli asset da tutelare, che da materiali sono diventati intangibili. I Security Manager agiscono al di fuori di ogni diretto interesse, con il buon senso, la correttezza morale e la coscienza di svolgere un compito che reclama un peculiare impegno e senso del dovere. Sono in possesso delle necessarie competenze per garantire la sicurezza generale, con l'obiettivo basilare di proteggere il business. Si pongono, dunque, come concreto riferimento per il management aziendale e gli *stakeholder*, in grado di agire in ogni area dell'impresa, offrendo un importante contributo sia all'interno che all'esterno dell'azienda.

Un progetto di sicurezza integrata

Il concetto contemporaneo di sicurezza che chiama in causa il Security Manager abbraccia un contesto molto ampio che va dalla sicurezza fisica dell'infrastruttura, al controllo della protezione delle strategie produttive dell'impresa, alla sicurezza delle infrastrutture critiche, alla sicurezza nazionale, alla sicurezza informatica, alla sicurezza sul lavoro, della fedeltà dei dipendenti, della rete di informazione-comunicazione, dell'introito merci, del trasporto protetto e sicuro dei prodotti, della privacy ecc.
È necessario, pertanto, realizzare un progetto di sicurezza integrata che gli esperti attueranno con l'analisi multidisciplinare e la valutazione di tutti i possibili rischi, unendo tutti gli ambiti aziendali e le loro interconnessioni, sulla base delle peculiari competenze in materia di: ***Crisis Management, Risk Analysis, Emergency Planning, Personnel Security, Physical Security, Protection of Sensitive Information, Loss prevention & Asset Protection, Investigations, Legal Aspects.*** Si tratta di discipline che consentono a un'azienda di prevenire rischi e ripristinare eventuali danni derivanti da azioni illecite e iniziative dolose.

I rischi dolosi e criminosi

È opportuno evidenziare che la legislazione europea e quella nazionale impongono al datore di lavoro di ogni attività produttiva di identificare e valutare tutti i rischi, non soltanto quelli accidentali e colposi, che potrebbero causare danni ai lavoratori durante lo svolgimento delle loro attività all'interno dell'azienda, ma anche quelli di origine volontaria e pertanto definibili dolosi e/o criminosi. Questa interpretazione, a seguito della condanna del 2002 nei confronti dell'Italia, da parte della Corte di Giustizia europea, per *"inadeguato"* recepimento di alcune direttive sulla sicurezza nei luoghi di lavoro, è stata, una volta per tutte, ribadita anche dal Testo Unico in materia di igiene e sicurezza nei luoghi di lavoro ***(ex artt. 17, 28 e 29 del D.Lgs. 81***

Security Management: 4 fasi fondamentali

Queste sono le 4 fasi fondamentali della fornitura dei servizi di Security Management:

- **Risk Assessment** | Mappatura dei rischi attraverso le fasi di analisi e valutazione.
- **Risk Reporting** | Presentazione dei rischi rilevati, stato attuale di gestione e classificazione delle risultanze delle precedenti fasi.
- **Risk Treatment** | Fase decisionale della scelta delle misure idonee a modificare il profilo del rischio (ad esempio evitarlo, ridurlo, accettarlo, trasferirlo...).
- **Risk Monitoring** | Valutazione critica del modo in cui i controlli sono concepiti, dei tempi e i modi in cui sono presi i provvedimenti necessari. Assicurazione che il sistema continui a funzionare efficacemente.

L'autore

Vincenzo Circosta, uno dei massimi esperti di Security sul territorio nazionale, è Consulente Sicurezza Anticrimine, Senior Security Manager UNI 10459:2017 ed Esperto in Scienze Criminologiche e Investigative.
È fondatore e socio di **Homeland Securnet**, società attiva nella sicurezza.

Il concetto di sicurezza

Il concetto di sicurezza, nel senso più ampio del termine, si fa solitamente coincidere con:

- **Safety**: sicurezza intesa come protezione delle risorse umane e delle risorse materiali, da pericoli derivanti da fenomeni naturali, accidentali o da errori umani.
- **Security**: sicurezza intesa come protezione delle risorse umane, delle risorse materiali e immateriali, da eventi di natura dolosa o colposa; cultura, studio e gestione della sicurezza per la concretizzazione di misure idonee per la prevenzione.
- **Emergency**: riguarda la protezione e il contenimento del pericolo: strutture che operano per fare Emergency sono le Forze di Polizia, i Vigili del fuoco, il soccorso medico d'emergenza.

Il punto d'incontro tra questi concetti è la tutela di persone e di beni, la qualità della vita e la creazione di una condizione di benessere.

del 9/04/2008 e s.m.i.). L'analisi del rischio *"crimine"* deve essere accurata, rigorosa e scientificamente corretta, tale da consentire la valutazione più oggettiva possibile del fenomeno, in vista dei conseguenti rimedi da adottare. L'esperto incaricato dell'analisi dovrà stilare una classifica della rischiosità di ciascuna unità produttiva dell'azienda tenendo conto di diversi ambiti:

- **l'azienda e le sue unità produttive;**
- **l'azienda e i suoi stakeholders;**
- **le altre aziende del settore e le rispettive unità produttive;**
- **la delittuosità (l'incidenza criminologica) delle aree geografiche di pertinenza;**
- **l'azienda e le infrastrutture critiche.**

Tali ambiti dovranno essere valutati anche in funzione del tempo, confrontando i valori del periodo precedente, ove, stabilita una ipotetica misurazione di pericolosità, la situazione va migliorando o peggiorando. La classifica del rischio di origine criminosa, inoltre, non sarà unica per ciascuna unità produttiva, ma sarà riferita per ogni tipo di delitto che può essere perpetrato ai danni dell'azienda, variando la frequenza a seconda delle aree geografiche, per cui una unità produttiva potrà essere ad elevato rischio rapina ma a basso rischio furto, al contrario di un'altra situata in una diversa area geografica. Con il termine di infrastruttura critica si intende un sistema, un processo, un insieme la cui distruzione, interruzione o anche parziale o momentanea indisponibilità hanno l'effetto di indebolire in maniera significativa l'efficienza e il funzionamento normale di un Paese e segnatamente la sicurezza delle aziende. Per infrastrutture critiche si intendono le risorse relative a: produzione, trasmissione e distribuzione dell'energia elettrica nonché le altre forme di energia (gas naturale); telecomunicazioni e telematica; risorse idriche e gestione delle acque reflue; agricoltura, produzione delle derrate alimentari e loro distribuzione; sanità e ospedali; trasporto aereo, navale, ferroviario, stradale e distribuzione dei carburanti e generi di prima necessità; banche e servizi finanziari; sicurezza, protezione e difesa civile.

L'analisi e la valutazione dei rischi

L'attività del Security Manager prevede un'accurata analisi e successiva valutazione dei rischi e dei pericoli di origine criminosa effettuate all'interno degli obiettivi esaminati, mediante sopralluogo in situ, con particolare attenzione ai rischi collegati a: furti, aggressioni/rapine, illeciti accessi, minacce provenienti dall'esterno, tentati incendi dolosi, azioni dimostrative e atti vandalici commessi dalla criminalità comune ovvero mirati ad azioni di manifestanti, nel corso di scioperi e/o tumulti socio-politici, oppure ancora collegati alle minacce terroristiche pervenute da parte di estremisti di matrice politico-religiosa. A seguito della suddetta analisi, il Security Manager fornirà i necessari suggerimenti migliorativi riguardanti le misure messe in atto o da attuare, finalizzate a ridurre la probabilità dell'accadimento dell'evento criminoso e, ove ciò non bastasse, a mitigare il danno.

Il concetto, diventato obbligo normativo ex artt. 17, 28 e 29 del D.Lgs. 81/2008 e s.m.i., di *"valutare tutti i rischi"* e quindi anche di quelli di origine criminosa, rende il datore di lavoro il vero soggetto responsabile, considerando anche i fattori soggettivi e personali come elementi necessari per integrare la valutazione. Pertanto egli deve potersi avvalere di specialisti in grado di consentirgli di ottemperare alle disposizioni legislative senza che si creino pericolose situazioni di incertezza.

L'individuazione e la descrizione dei rischi più frequenti e le misure di prevenzione e protezione per la loro riduzione sarà argomento del mio prossimo articolo.