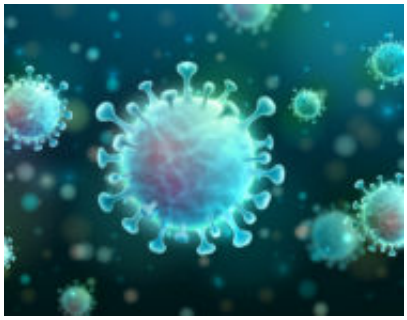
Medical Security: nuove sfide di sicurezza a fronte di nuove minacce globali

Author : Giovanni Villarosa

Date : 26 Marzo 2020



> *“Colui che conosce solo il proprio lato della questione, ne conosce ben poco”.*
> John Stuart Mill

Il nuovo virus *nCoV2019*, il cd. *Coronavirus*, scoperto nella circoscrizione cinese di Wuhan, oltre a suscitare l'ancestrale timore di una **pandemia planetaria** trasmette una sensazione ancora più subdola: il mistero della sua non chiara natura.

Diversi esperti di ***intelligence*** **e** ***security*** impegnati nel settore della **biosicurezza** hanno analizzato sin ora una mole tale di dati da fonti Osint su ogni aspetto di *medical security* e di *crisis management* riguardante il nuovo fenomeno diffusivo del **virus,** ma siamo ancora lontani da risultati certi e condivisi.

Tanto gli esperti, quanto *mass media* e *social*, hanno dato ampia risonanza alla scoperta del virus, prefigurando diversi scenari, fino ad arrivare persino al il più controverso: la possibilità che **Covid-19** sia una bioarma orfana**,** rilasciata **(?)** da un laboratorio classificato *BSL-4 level* (massimo livello di biocontenimento), installazione presente a Whuan, area dell’epicentro epidemico.

Congetture a parte, per il momento l’unica cosa certa è che siamo nel pieno di una crisi biosanitaria, emergenza globale nata intorno al nuovo virus, che preoccupa ogni giorno di più i governi centrali, per gli impatti negativi che si potranno avere sul lungo periodo su scala economica e sociale, sui sistemi produttivi, l’incolumità e la salute delle persone.

Del resto, nelle organizzazioni aziendali, sia pubbliche che private, proprio in momenti critici come quelli che sta vivendo il nostro Sistema Paese, purtroppo, si materializza la vera occasione per testare, analizzandole, le **capacità resilienti** della propria struttura organizzativa, le policy e le procedure di ***security, emergency*** **e** ***safety***, elaborate a protezione della vita dei propri dipendenti e dell’intero patrimonio aziendale.

Ora, per fronteggiare questa **emergenza globale** ogni datore di lavoro - pubblico o privato che sia - è vincolato per legge ad adottare, tramite il medico del lavoro, tutte le **misure protettive e preventive** necessarie per garantire i lavoratori, creando condizioni idonee per svolgere le attività in modo sicuro.

Infatti, quando le aziende, e le stesse istituzioni, operano in zone classificate **a rischio** - nella fattispecie, sanitario - devono adottare severe *policy* di *risk management* (misure di contenimento del rischio, sospensione dei viaggi/missione, rimpatrio del personale, etc) da e per le cd. zone ***hotspot***, per ridurre i pericoli da esposizione alle minacce sanitarie, o fisiche che siano, intrattenendo un **filo diretto** e costante con il Ministero della Sanità, per le procedure di *safety* da adottare nell'immediatezza dei casi, e con la Farnesina (AISE) per le operazioni di *security* nel momento del rimpatrio.

Altra caratteristica fondamentale per la prevenzione e la tutela della salute e dell'incolumità del dipendente in missione, è quella di fornirgli **adeguate informazioni** circa i modelli comportamentali da seguire sul luoghi operativi fuori area, definendo un **piano informativo strutturato**, dati contenuti anche nelle schede Paese consultabili sul sito degli Affari Esteri.

Con mercati sempre più **interconnessi e interdipendenti,** che vede moltissime aziende proiettate fuori dai confini nazionali, ogni settore economico strategico, inevitabilmente, è costretto ad affrontare con maggior frequenza questi nuovi rischi sanitari correlati alla trasferta dei propri lavoratori.

Prestazioni di lavoro, quelle fuori dai confini, classificate nell'ambito delle linee guida della Società Italiana di Medicina del Lavoro come attività *"atipica che presenta flessibilità di impiego ed è caratterizzata, oltre che dai rischi della mansione, da fattori correlati alle condizioni di soggiorno del paese ospitante".*

Orbene, in un'ottica di adempimento ai disposti legislativi sulle misure di sicurezza a garanzia dell'incolumità del dipendente (TU 81/08), ci si pone davanti sempre lo stesso interrogativo: è compito del datore di lavoro proteggere il dipendente, durante lo svolgimento delle sue mansioni, da tutte quelle attività, esogene e/0 endogene, dolose e/o colpose, a cui lo stesso viene esposto?

La risposta, decisamente scontata, è scritta appunto nel D.Lgs 81 e rafforzata dall'art.18 del D.Lgs n° 151/2015 : responsabilità oggettiva, civile e penale, del datore di lavoro, sia esso pubblico che privato, ma soprattutto analisi dei rischi, degli atti ostili e criminali, l'elaborazione di piani di emergenza ed evacuazione, l'analisi della normativa antinfortunistica locale e delle interrelazioni con quella italiana, pianificazione, organizzazione, coordinamento e gestione della trasferta secondo le prassi contenute nello standard ISO 31030.

Una norma ISO che delinea le *compliance* del ***Duty of Care***, conformità specifica per la gestione dei cd. **rischi da trasferta**, linee guida che dettano gli strumenti per dimostrare, anche in sede giudiziaria, di aver fatto materialmente tutto il possibile (D.Lgs 231/2001), contro ogni ragionevole dubbio.

Ma per mettere in atto tutte queste misure di protezione e garanzia, quali contromisure vanno poste in atto, e quali figure organizzative andranno coinvolte?

Le risposte sono diverse; inizialmente va interessato e coinvolto l'ufficio del *Security Manager,* che affronterà tutte le attività di *safety e security* (*safety* e *security management, travel risk, medical security*, etc.) che coinvolgano, in maniera diretta o indiretta, il personale dipendente impegnato.

Tuttavia, oltre ai rischi di sicurezza legati alla specifica mansione esercitata, si dovranno valutare anche i nuovi rischi emergenti di *medical security* (igiene, supporti sanitari di emergenza, ricoveri locali, esfiltrazione sanitaria, etc.) legati all'area del Paese ospitante; dunque, Security Manager, RSPP e medico competente in sinergia tra loro, e su preventive informazioni rese dal datore di lavoro, gestiranno tutti gli aspetti legati alla salute e alla sicurezza in operazioni fuori area.

Ma il mutato **scenario internazionale**, come si è visto in questi giorni virulenti, impone sempre più specifiche precauzioni e conoscenza del quadro sovranazionale, non solo a livello geopolitico: difatti, alla luce di quanto accaduto, d'ora in avanti tutta la problematica degli spostamenti esteri andrà programmata secondo nuovi processi di *medical security*, che supportino fattivamente i piani di *travel security*.

Processi che dovranno trovare riferimenti stabili nelle *capability* contenute *nella medical intelligence* **(*Medint*)** che, come tutte le attività di *intelligence*, si articola nelle tipiche fasi di raccolta delle informazioni sanitarie della nazione interessata e di analisi dei dati raccolti, per delineare verosimilmente più scenari possibili, rilasciando un prodotto informativo che gli uffici di sicurezza aziendale inseriranno nelle relative schede Paese.

Ma per una corretta compilazione delle prescrizioni di sicurezza in uso al personale che sarà impiegato fuori dal territorio nazionale, a differenza di altre informazioni, la *medical security* richiede una consolidata competenza medica nelle fasi di gestione e trattazione del ciclo informativo ricevuto (ospedali, malattie, igiene pubblica, epidemie, farmaci, etc.).

Ecco allora come l'azione sinergica tra *Security Manager*, RSPP e medico competente diventa fondamentale per la costruzione di un sistema di protezione individuale dei dipendenti, e un indiretto ritorno positivo a tutto vantaggio delle iniziative economiche strategiche per gli uffici che gestiscono le azioni di *business intelligence*.

In ultimo, l'attuale crisi pandemica ha mostrato anche l'altra faccia della medaglia: quella del pericolo da **epidemia tecnologica,** che dovrà indurci ad attente riflessioni, perché dopo la grande crisi economio-finanziaria mondiale dovuta al drammatico **attentato 9/11** alle Torri Gemelle, che cambiò la percezione del pericolo nella società globale, anche questa nuova e subdola vulnerabilità (sociale, psicologica, tecnologica) classificata come **epidemia cyber** avrà negative ripercussioni sul sistema socio-finanziario mondiale.

Infatti, mentre il virus continua la sua inarrestabile cavalcata contagiosa sulla società, di pari passo sul web cresce esponenzialmente l'**infezione** da ***malicious attacks*** (*intrusion, malware,*

phishing), sfruttando vantaggiosamente le **deficienze** di sicurezza delle reti (*cyber security*).

Le prime avvisaglie la **Polizia di Stato** **(CNAIPIC)** le ha già intercettate, lanciando un preciso allarme ai tentativi di truffe informatiche testate in rete in questi ultimi giorni, con pesanti attività di *phishing* legate al **Covid-19.**

D’altronde le infrastrutture **Telco**, wireless o cablate che siano, utilizzate dalla **sanità moderna** rimangono il mezzo **informativo** centrale nella lotta all’epidemia; non voglio immaginare neanche per un istante quale catastrofe potrebbe accadere se un ospedale, un sito farmaceutico o altri centri fondamentali per la sanità pubblica dovessero cadere sotto i colpi di un pesante attacco cyber!

Articolo a cura di **Giovanni Villarosa**