Il lavoro da remoto e i problemi di sicurezza

Le buone pratiche per Smart Working e Telelavoro

*di Antonio Campodipietro**

Come abbiamo potuto sperimentare in questo periodo, una pandemia, forse più di altre situazioni di crisi, può avere effetti rilevanti sulle aziende: è un evento che, oltre causare problematiche legate alla salute, può interrompere le attività e i processi aziendali. Un *Piano Pandemico*, da adottare all'inizio della diffusione del *SARS-CoV-2*, sarebbe stato utile per le aziende; purtroppo la maggioranza delle PMI in Italia non ne avevano uno pronto.
Fortunatamente, molte **aziende dell'*Information Technology***, per aumentare la produttività, da tempo fanno un importante uso delle **tecnologie** che rendono semplice il **lavoro da remoto**. Questo strumento offre anche un altro vantaggio: consentire il lavoro da remoto nel corso di un evento critico è una **pratica di resilienza prevista nei Piani di Continuità Operativa**.
La disponibilità di queste tecnologie ha quindi permesso a molte realtà di non interrompere totalmente le proprie attività. Tuttavia, si sono presentate **problematiche di sicurezza**, sia dal punto di vista della **salute sul lavoro (*safety*)** sia da quello della **sicurezza delle informazioni (*security*)**. Per risolvere queste problematiche sono fondamentali politiche e prassi efficaci in modo che il lavoro da remoto risulti non solo pratico ma anche sicuro.

LA SICUREZZA SUL LAVORO (*SAFETY*)

Il lavoro da remoto, cioè l'attività effettuata fuori dai locali dell'azienda, può essere regolato contrattualmente **in due diverse modalità**: come ***Telelavoro***, dove l'attività è svolta con l'orario tipico da una postazione stabilita (tipicamente presso l'abitazione del dipendente) oppure come ***Lavoro Agile* (*Smart Working*)**, dove invece l'orario non è vincolato (poiché

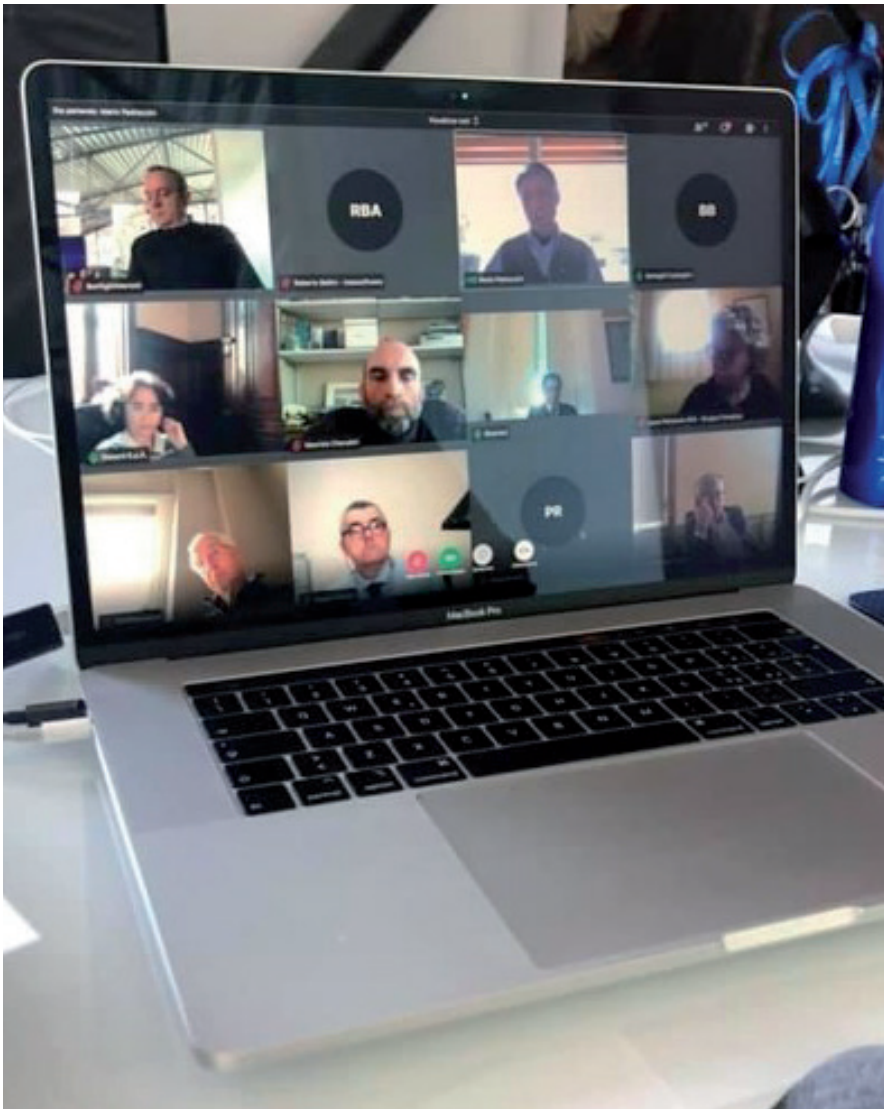
* ADS Spa

l'attività è legata agli obiettivi da raggiungere) e non è prevista una postazione fissa.
Per quanto riguarda la sicurezza sul lavoro, **entrambe le tipologie contrattuali** devono tener presente dell'art.3 c.10 del **D.Lgs 81/08**, il quale prevede che "*a tutti i lavoratori subordinati che effettuano una prestazione continuativa di lavoro a distanza, mediante collegamento informatico e telematico*" si applicano ugualmente le disposizioni riguardanti le *attrezzature munite di videoterminali* e quelle per l'*uso delle attrezzature di lavoro e dei dispositivi di protezione individuale*. In pratica, nel lavoro a distanza, permane l'obbligo dell'**analisi dei posti di lavoro** (con particolare riguardo ai **rischi per la vista** e per gli occhi, ai problemi legati alla **postura** ed all'affaticamento fisico o mentale e alle **condizioni ergonomiche e di igiene ambientale**) nonché quello di prendere le misure necessarie per "salvaguardare i lavoratori da **tutti i rischi di natura elettrica**".
Quindi per il lavoro remoto rimane necessaria l'adozione delle **misure appropriate per ovviare ai rischi riscontrati nel DVR** (Documento di valutazione dei rischi) nonché l'organizzazione e predisposizione dei posti di lavoro: la valutazione deve tenere in considerazione "*le condizioni e le caratteristiche specifiche del lavoro*" (comprese eventuali interferenze) e i "*rischi presenti nell'ambiente di lavoro*".
È posta anche attenzione sulla necessità di **verificare la corretta attuazione della normativa** in materia di "tutela della salute e sicurezza da parte del lavoratore a distanza" per cui è possibile, previo preavviso e consenso del lavoratore, l'accesso ai locali per i controlli opportuni.
Ricapitolando, **l'attivazione del lavoro da remoto pone alle aziende delle problematiche di sicurezza sul lavoro che dovranno essere valutare nel proprio DVR**. Ma questa doverosa valutazione dei rischi riguardante la tutela della **salute dei dipendenti** in realtà torna utile anche dal punto di vista dell'operatività aziendale: gli standard internazionali che si occupano di *Security* e di Continuità Operativa considerano **le persone come risorse importanti per attuare i propri piani di sicurezza delle informazioni** e quindi fra le prime da tenere presente in un'analisi dei rischi.

LA SICUREZZA DELLE INFORMAZIONI (*SECURITY*)

Per la sicurezza delle informazioni sono disponibili più ***framework* internazionali di riferimento**: quale scegliere per il proprio sistema di gestione? È presente uno spunto nell'art.32 *Sicurezza del trattamento* del *GDPR* che richiede di mettere "*in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso… la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento*".

Il richiamo a due serie di standard ISO è evidente: la **ISO/IEC 27000** definisce la ***sicurezza delle informazioni*** (3.28) come la protezione della **riservatezza** (3.10), cioè l'accesso controllato per garantire la confidenzialità, dell'**integrità** (3.36), cioè la completezza e la correttezza, e della **disponibilità** (3.7), cioè la possibilità di accedere quando necessario. Per quanto riguarda invece la **resilienza**, il termine compare già nel titolo della **ISO 22300** (*Security and resilience*) ed è definita come la capacità di assorbire e adattarsi in un ambiente che cambia (3.193.2).
Entrambe le serie ISO offrono, in standard certificabili, indicazioni riguardo le **persone** sia nella gestione della **sicurezza delle informazioni** che in quella della **continuità operativa**: nella **ISO/IEC 27001** (*Sistemi di gestione della sicurezza delle informazioni*) i controlli previsti si occupano, fra l'altro, della sicurezza delle persone (A.7) e di quella degli ambienti di lavoro (A.11); nella **ISO/IEC 22301** (*Sistemi di gestione della continuità operativa*) viene chiesto di identificare non solo i **rischi** connessi all'interruzione delle attività prioritarie e dei processi, ma anche ad un elenco di risorse fra cui ci sono **le persone** (8.2.3).
Inoltre, riguardo la **sicurezza delle informazioni nel lavoro remoto**, sono fornite anche delle guide.
La più dettagliata è presente nella **ISO/IEC 27002** (*Raccolta di prassi sui controlli per la sicurezza delle informazioni*) dove, nel paragrafo dedicato all'argomento dal titolo ***Telelavoro*** (6.2.2), è indicata la necessità di una **politica e di misure di sicurezza per proteggere le informazioni gestite presso i siti di telelavoro**, tenendo conto di vari fattori, fra i quali: il livello di sicurezza fisica dei locali, la sicurezza delle comunicazioni, la fornitura di VDI per non memorizzare informazioni su eventuali dispositivi privati, il pericolo della riservatezza riguardo altri inquilini (familiari, conviventi o amici), l'uso di reti casalinghe e dei servizi *wireless*, intese per concordare i diritti di autore per sviluppo su eventuali dispositivi privati nonché l'autorizzazione di un accesso su questi per indagini di sicurezza e, infine, i sistemi di protezione quali *anti-malware* e *firewall*.
Mentre nella **ISO/IEC 22313** (*Sistemi di gestione per la continuità operativa - Linee guida*), viene indicata **la possibilità di "lavorare da casa o in siti remoti"** (8.3.2.4) fra le **strategie aziendali** "per ridurre l'impatto dell'indisponibilità della sua normalità" dell'ambiente di lavoro standard.
Ricapitolando, **le politiche di sicurezza delle informazioni devono predisporre misure per gestire il lavoro da remoto** in maniera corretta: gli standard internazionali rappresentano uno strumento molto utile per elaborare queste politiche.



IL LAVORO DA REMOTO COME STRATEGIA DI SICUREZZA

L'inaspettato *lockdown* ha costretto molte aziende a improvvisare velocemente un piano per il lavoro da remoto. Per la *fase 2*, ma anche in prospettiva futura, è auspicabile che si vada oltre l'improvvisazione, istituendo una vera e propria **politica per il lavoro da remoto**; questa deve essere **conforme alla normativa nazionale sulla sicurezza sul lavoro** e **coerente con il proprio sistema per la sicurezza delle informazioni**, divenendo anche **strategia per la Continuità Operativa**: la *sicurezza delle informazioni* è un paradigma per il *lavoro da remoto*, ma a sua volta il *lavoro da remoto* è uno strumento per la *sicurezza delle informazioni*.