ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Ordine degli Ingegneri della provincia di Napoli

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

Convegno – La comunicazione digitale nell'organizzazione degli studi professionali: opportunità e pericoli legati all'uso delle reti

Smart Working: modelli organizzativi, rischi e potenzialità

Ing. Luca Del Pizzo, Ph.D.

Lo Smart Working oggi…

- Milioni di persone nel mondo hanno sperimentato per la prima volta negli ultimi mesi la possibilità di **essere produttivi anche senza recarsi in ufficio.**
- **Anche le aziende un tempo indifferenti a questa modalità di lavoro ne hanno compresso i vantaggi.**
- Molte aziende stanno valutando di **mantenere il lavoro agile** anche dopo lo stato di emergenza.
- Questo porta ad una **trasformazione delle aziende** e quindi dell'**intera società.**
- Per raggiungere questo obiettivo concreto, bisogna provvedere ad una **riorganizzazione**, a valutare la **sicurezza ICT e la protezione dei dati personali trattati**, l'utilizzo di **strumenti digitali adeguati**, la valorizzazione del **benessere dei dipendenti** e la diffusione della **cultura digitale** in tutti gli ambiti aziendali.

Smart working: definizione

- Lo **smart working (o lavoro agile)** è una modalità di esecuzione del rapporto di lavoro subordinato caratterizzato **dall'assenza di vincoli orari o spaziali** e un'organizzazione per **fasi**, **cicli** e **obiettivi**, stabilita mediante **accordo tra dipendente e datore di lavoro**;
  - una modalità che aiuta il lavoratore a conciliare i tempi di vita e lavoro e, al contempo, favorire la crescita della sua produttività.

- La **definizione di *smart working***, contenuta nella legge n. 81/2017, pone l'accento sulla **flessibilità organizzativa**, sulla **volontarietà** delle parti che sottoscrivono l'accordo individuale e sull'utilizzo di **strumentazioni** che consentano di lavorare da remoto (come, ad esempio, pc portatili, tablet e smartphone).
  - Capo II, art. 18, L. 81/2017
    https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2017-05-22;81!vig=

Smart working: definizione

Capo II

LAVORO AGILE

Art. 18

Lavoro agile

1. Le disposizioni del presente capo, allo scopo di incrementare la competitivita' e agevolare la conciliazione dei tempi di vita e di lavoro, promuovono il lavoro agile quale modalita' di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attivita' lavorativa. La prestazione lavorativa viene eseguita, in parte all'interno di locali aziendali e in parte all'esterno senza una postazione fissa, entro i soli limiti di durata massima dell'orario di lavoro giornaliero e settimanale, derivanti dalla legge e dalla contrattazione collettiva.

2. Il datore di lavoro e' responsabile della sicurezza e del buon funzionamento degli strumenti tecnologici assegnati al lavoratore per lo svolgimento dell'attivita' lavorativa.

Portale Servizi Lavoro

- Ai lavoratori agili viene **garantita la parità di trattamento** – economico e normativo – rispetto ai loro colleghi che eseguono la prestazione con modalità ordinarie. È, quindi, prevista la loro **tutela in caso di infortuni e malattie professionali**, secondo le modalità illustrate dall'INAIL nella Circolare n. 48/2017.

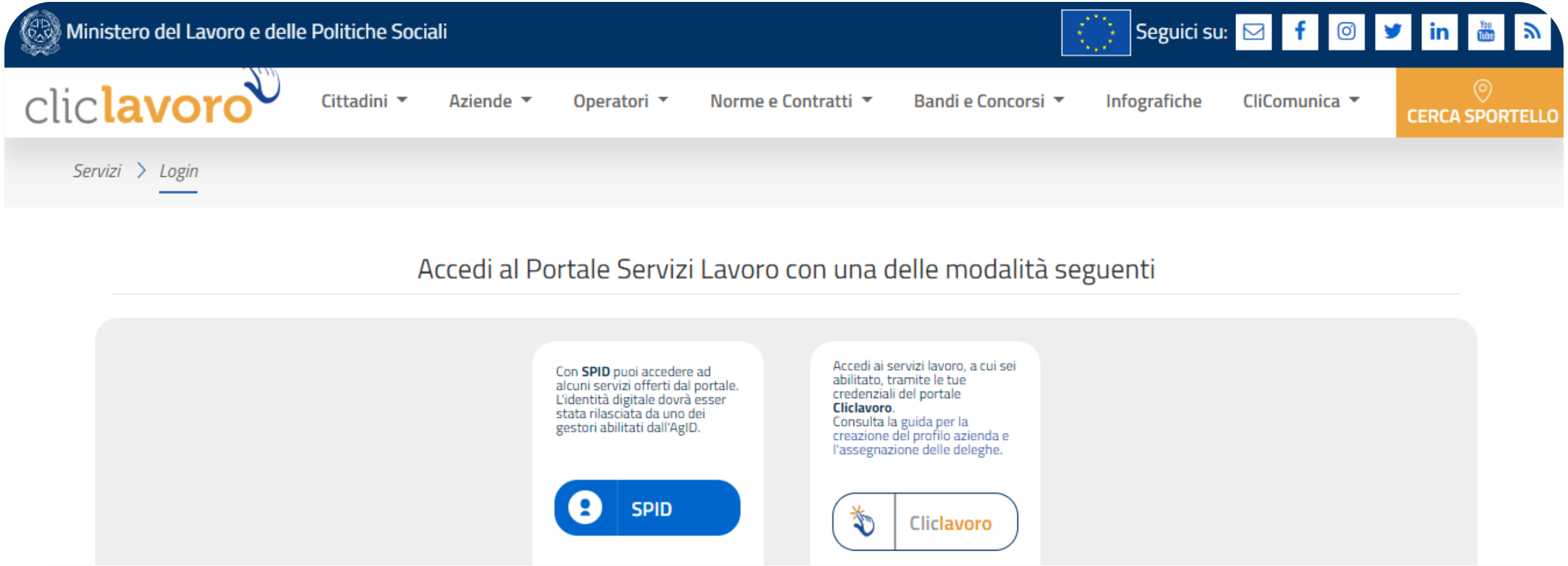
- A partire dal 15 novembre 2017, le aziende sottoscrittrici di **accordi individuali di smart working** possono procedere al loro invio attraverso l'apposita piattaforma informatica messa a disposizione sul portale dei servizi del **Ministero del Lavoro e delle Politiche Sociali**.

Portale Servizi Lavoro

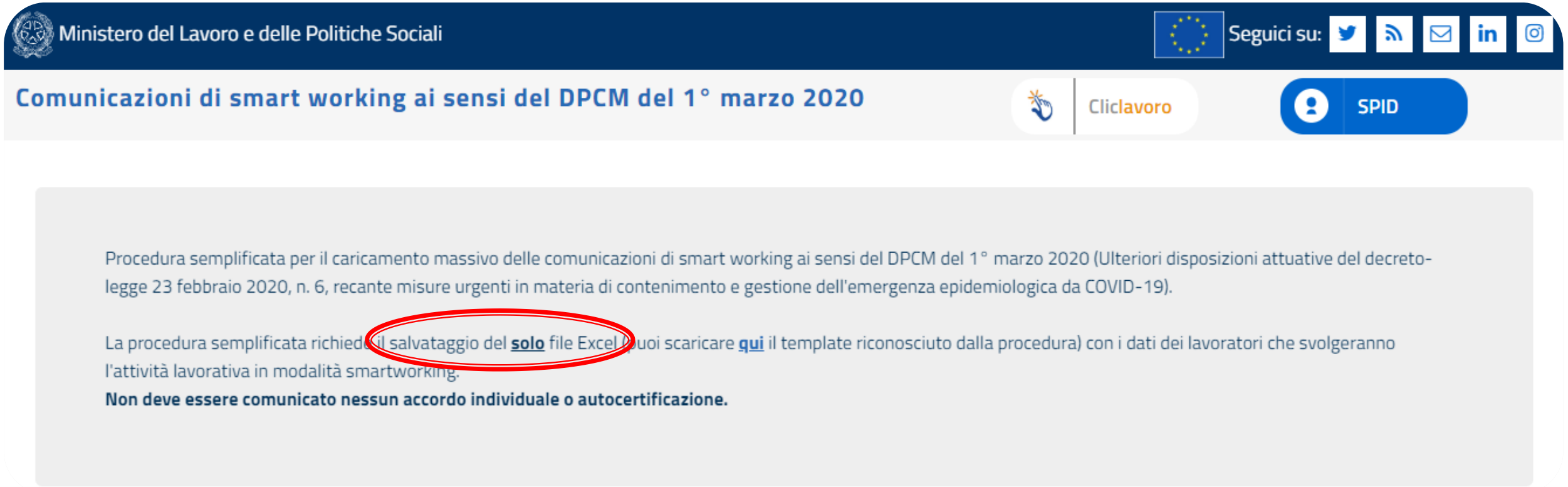
- Per accedere sarà necessario possedere SPID (Sistema Pubblico di Identità Digitale).

- Nell'invio dell'accordo individuale dovranno essere indicati i dati del datore di lavoro, del lavoratore, della tipologia di lavoro agile (tempo determinato o indeterminato) e della sua durata.

Portale Servizi Lavoro



Portale Servizi Lavoro



ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Ordine degli Ingegneri della provincia di Napoli

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

L'Accordo di Smart Working

- Di norma deve essere in **forma scritta** e deve contenere almeno questi **contenuti minimi**:
  - **durata**: a tempo indeterminato o determinato;
  - **preavviso**: il recesso è possibile con un preavviso di almeno 30 giorni (90 per i lavoratori disabili) per gli accordi a tempo indeterminato o in presenza di un giustificato motivo;
  - esecuzione della prestazione lavorativa al di fuori dei locali aziendali, con particolare riguardo agli **strumenti tecnologici utilizzati** e al **rispetto del diritto alla disconnessione** per il lavoratore;
  - **controllo** della prestazione lavorativa all'esterno dei locali aziendali, tenendo conto dell'articolo 4 dello Statuto dei Lavoratori.

Lavoro Agile vs. Telelavoro

- Nello Smart Working il lavoro è svolto **senza una postazione fissa**: può essere all'esterno dei locali aziendali o al loro interno.

- Nel telelavoro il dipendente **lavora generalmente da casa** e nel contratto può essere specificata la necessità di raggiungere il posto di lavoro tradizionale una volta alla settimana, o in base agli accordi presi.

- Nello Smart Working è presente il **diritto alla disconnessione**: tra l'azienda e il dipendente devono essere stabilite misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro.

Vantaggi dello Smart Working

Riduzione dei costi aziendali per gli spazi da adibire a ufficio

Crescita della produttività

Riduzione dei tempi di trasferimento da casa a ufficio

Diminuzione dell'inquinamento atmosferico

Migliore bilanciamento tra tempi di vita-lavoro (work-life balance)

Aumento della motivazione e soddisfazione lavorativa

Conviene sia alle Organizzazioni che ai Dipendenti!!!

Secondo l'Osservatorio Digital Innovation del Politecnico di Milano, l'adozione di un progetto strutturato di Smart Working può produrre un **incremento di produttività pari a circa il 15% per lavoratore**.

Criticità dello Smart Working

Opportunità dello Smart Working

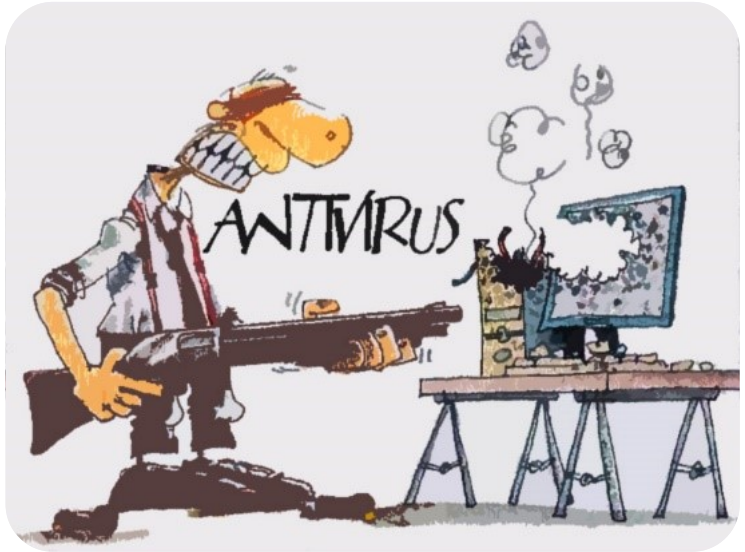
Maggiore ingaggio dei giovani

Migliore gestione dei picchi di volume non prevedibili

Carriera basata su obiettivi

Minacce dello Smart Working

- Diminuzione dei rapporti interpersonali
- Uso improprio dei dispositivi
- Tecnologie non adeguate
- KPI non adeguati o non facilmente controllabili



Il Progetto dello Smart Working

- Introdurre lo smart working in azienda significa attuare un **progetto** che coinvolga tutti i settori e tutte le componenti interessate.
- Il progetto deve partire da un'attenta considerazione degli **obiettivi**, delle **priorità** e delle peculiarità **tecnologiche**, **culturali** e **manageriali** dell'organizzazione.

- **Obiettivo**: applicare tecnologie avanzate per connettere persone, spazi, oggetti ai processi di business, per aumentare la produttività, innovare e coinvolgere le persone.

Alcune aree di intervento per implementare lo Smart Working

Bisogna pianificare una strategia di Smart Working!!!

Per ottenere un'evoluzione dei modelli organizzativi aziendali si deve prevedere una **roadmap** dettagliata fase per fase.

Alcune aree di intervento per implementare lo Smart Working

Vengono definiti gli **obiettivi**, analizzati i **rischi**, definite le **metriche**, individuati gli **strumenti** operativi più adatti, definite delle **policy**, redatti gli **accordi** tra le parti e innanzitutto gli attori coinvolti devono essere **formati** all'utilizzo delle **nuove modalità operative**.

I rischi del digitale

- Molte aziende stanno valutando di **mantenere il lavoro agile** anche dopo l'emergenza Covid-19.

- Con la pandemia il lavoro a distanza ha fatto **aumentare i rischi** dovuti soprattutto alla mancanza di una formazione adeguata sugli strumenti utilizzati.

- **Come evitare perdite e intrusioni?** Adottare un approccio di sicurezza focalizzato sulle persone e sulla loro protezione. Bisogna sensibilizzare e formare il personale.

Cyber rischi… quando il nemico è in casa

- I cybercriminali sfruttano l'aumento dello *smart working* per penetrare le difese informatiche di aziende e utenti.

Ai fini di questa ricerca, le minacce interne sono definite come segue:

- Dipendente o sub-appaltatore negligente;
- Utente interno malintenzionato
- Ladro di credenziali d'accesso

Per esempio, le minacce interne sono costate alle aziende 11,45 milioni di dollari nel 2020, un aumento del 31% dagli 8,76 milioni di dollari del 2018 (Ponemon). Inoltre, il numero di incidenti è aumentato del 47% in soli due anni, dai 3.200 del 2018 (Ponemon) ai 4.716 del 2020. Questi dati mostrano che le minacce interne sono un rischio per la sicurezza informatica ancora attuale, anche se spesso non adeguatamente affrontato dalle aziende rispetto alle minacce esterne.

Cyber rischi… quando il nemico è in casa

- Il furto delle credenziali sono ¼ degli incidenti
- **2,79 milioni di dollari** il costo annuale per le aziende
- I dipendenti imprudenti, causa di oltre il **60%** degli incidenti, hanno portato a perdite per **4,58 milioni di dollari**.
- Nel rapporto si evidenzia come la **posta elettronica** sia il canale privilegiato dai criminali informatici.
- Su **3.500 dipendenti** di grandi aziende, il **55%** ha subito nell'ultimo anno un attacco di phishing e il **33%** è stato vittima di ransomware.

Per proteggere le organizzazioni occorre partire dalle persone!!!

Un caso concreto: l'utilizzo dei dispositivi personali

- Non tutti i dipendenti hanno ricevuto in tempo utile un laptop o uno smartphone, e in diversi casi le aziende non hanno le risorse per fornire a tutti i dipendenti i dispositivi.
  - Ciò significa che in alcuni casi ai lavoratori **è stato chiesto di utilizzare i propri dispositivi per motivi di lavoro**.
- In altri casi le aziende hanno attivato un **team di sicurezza** per configurare adeguatamente i dispositivi prima di consegnarli ai dipendente
  - Ad es. black list di software installabile, porte USB bloccate, …
- Poiché il team di sicurezza **non è in grado di monitorare** ogni singolo dispositivo personale, non saprà se tali dispositivi utilizzano software e sistemi operativi aggiornati oppure se presentano altre **vulnerabilità** che potrebbero mettere a rischio le informazioni e i dati personali trattati.

Alcune soluzioni per le aziende

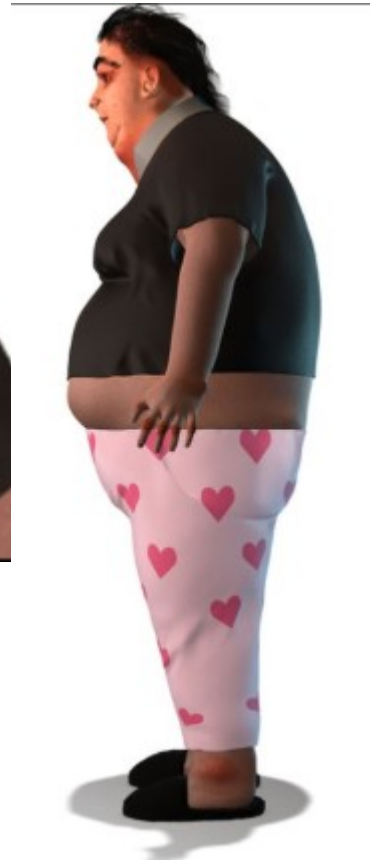
- **Autenticazione a più fattori** con password più *token*, smartphone o biometria;
- Sistemi di ***Identity and Access Management*** per garantire l'accesso solo alle risorse necessarie e con una visibilità limitata al ruolo;
- **Cifratura** di tutte le comunicazioni e dei file (ad es. VPN);
- ***Analytics e machine learning*** per analizzare i pattern di accesso e individuare connessioni sospette;
- **Politiche di sicurezza** per stabilire qual è il livello di accesso di cui ogni utente ha bisogno per eseguire uno specifico compito, in modo da limitare il rischio di visibilità eccessiva.

Rafforzamento della rete aziendale

- Nel periodo lockdown la rete Internet ha retto al consistente aumento di traffico (molti nodi di interscambio sono passati da una media annuale di 500 Mbps a 1 Tbps)
- Non per tutte le reti aziendali però sono riuscite a fronteggiare l'improvviso aumento della richiesta di banda
  - Ad esempio molte aziende non sono riuscite a far fronte alle richieste di connessioni VPN.
  - Il ricorso ad applicazioni in CLOUD può sicuramente alleviare il problema, ma non sempre è possibile (es. informazioni riservate o particolari categorie di dati personali).
  - Per questo è fondamentale potenziare la rete aziendale e pianificare le risorse in modo da poter gestire situazioni critiche, anche effettuando simulazioni e test.

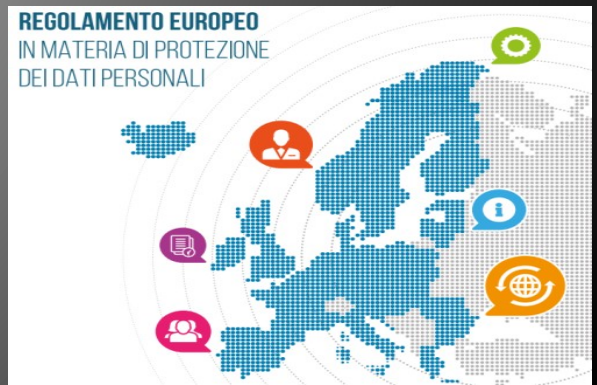
Oltre ai rischi digitali…

- Lei è Susan ed è la rappresentazione computerizzata di una persona che per 25 anni lavora da remoto.
- Susan è l'esito di uno studio americano promosso dalla società DirectlyApply che mette in guardia dai rischi dello smart working. Il lavoro condotto da un team di psicologi ed esperti di fitness ha portato a evidenziare gli effetti che il lavoro da remoto può causare sulla salute fisica e mentale nell'arco di 25 anni.
- Se non vengono prese misure necessarie ciò che può accadere non è lontano dall'immagine di Susan: occhi arrossati, infiammati e asciutti, problemi di obesità, problemi di calvizie, ferite recidive dovute alla continua azione del digitare sui tasti, spalle arrotondate e gobbe.



Fonte: https://www.tgcom24.mediaset.it/magazine/foto/ti-piace-lo-smart-working-ecco-come-

GDPR e Obbligo della Formazione del Personale



Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

GDPR

Il “Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016”, ha l’obiettivo di garantire una disciplina sulla protezione dei dati personali uniforme ed omogenea in tutta la UE

24 maggio 2016

Il **Regolamento entra in vigore;** i Paesi dell’Unione Europea avranno **due anni per porre in essere gli adeguamenti richiesti dalla normativa** in questione alle proprie politiche per la protezione ed il trattamento dei dati personali

25 maggio 2018

Il **Regolamento è definitivamente applicabile in via diretta in tutti i Paesi UE**, considerato che **non vi è la necessità di recepimento con atti nazionali** (anche se non poche disposizioni lasciano liberi gli Stati Membri - o richiedono agli stessi - di introdurre ulteriori regole e condizioni)

1. Definizioni
2. Ambito di applicazione territoriale
3. Autorità di controllo
4. Comitato europeo protezione dei dati
5. Principi applicabili al trattamento
6. Interessato
7. Diritti dell’interessato
8. Titolare del trattamento
9. Principio di accountability
10. Privacy by design e by default
11. Contitolari del trattamento
12. Responsabile del trattamento
13. Persone autorizzate al trattamento
14. Certificazioni
15. Sicurezza del trattamento
16. Data breach
17. Registri delle attività di trattamento
18. Valutazione impatto protezione dei dati (PIA)
19. Responsabile della protezione dei dati (DPO)
20. Trasferimento di dati extra UE
21. Nuovi diritti: Diritto all’oblio, Data portability
22. Cooperazione e coerenza
23. Mezzi di ricorso
24. Diritto al risarcimento e responsabilità
25. Disposizioni relative a specifiche situazioni di trattamento
26. Disposizioni finali
27. Sanzioni amministrative pecuniarie

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Formazione per il GDPR

- Il Regolamento prevede **l'obbligo della formazione** per le pubbliche amministrazioni ed imprese in materia di protezione dei dati personali per tutte le figure presenti nell'organizzazione (sia dipendenti che collaboratori).

- L'**art. 29** del regolamento prevede che "il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali **non può trattare tali dati se non è istruito** in tal senso dal titolare …".

- La centralità della formazione è confermata anche dall'**art. 32** "Sicurezza del trattamento" paragrafo 4 che prevede che "il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali **non tratti tali dati se non è istruito** in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Formazione per il GDPR

- Il **Garante**, in diversi casi, in sede ispettiva ha richiesto di acquisire il **programma ed il piano di formazione**, le dispense, i materiali erogati, il test finale ed ha analizzato le istruzioni fornite agli autorizzati al trattamento.
  - Ad esempio in riferimento all'accesso, alla consultazione delle banche dati, ai livelli di autorizzazione e delle policy aziendali (ad esempio in materia di password aziendali e di videosorveglianza).

- Bisogna **pianificare** quanto prima un **percorso ed un piano di formazione!**

Ing. Luca Del Pizzo, Ph.D.
ing.lucadelpizzo@gmail.com

Il progetto LamiaSicurezza.it

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI CASERTA

Ordine degli Ingegneri della provincia di Napoli

ORDINE DEGLI INGEGNERI DELLA PROVINCIA DI SALERNO

Grazie per l'attenzione

Convegno – La comunicazione digitale nell'organizzazione degli studi professionali: opportunità e pericoli legati all'uso delle reti

Smart Working: modelli organizzativi, rischi e potenzialità

Ing. Luca Del Pizzo, Ph.D.

ing.lucadelpizzo@gmail.com