COMUNE DI PINCARA
PROVINCIA DI ROVIGO
Via G. Matteotti, 287
Cod. Postale 45020
Telef. 0425. 745100 - Telefax 0425.745058
E-mail pincara@comune.pincara.ro.it
Cod. Fisc. 8200053.029.3
Part. IVA 0023352.029.5

Lavoro agile e sicurezza dei dati personali

Premessa

L'Italia, per arginare l'epidemia del Coronavirus, è ricorsa al lavoro agile grazie al Decreto attuativo approvato d'urgenza dal Governo, anche senza un accordo preventivo con i dipendenti, come richiesto, invece, dalla Legge del 2017.

Come risposta diretta alla situazione di emergenza che sta affrontando il nostro paese **il decreto non specifica né prescrive particolari adempimenti in termini di sicurezza dei dati personali** circa l'improvviso utilizzo dei BYOD (è un'espressione usata per riferirsi alle politiche aziendali che permettono di utilizzare i propri dispositivi personali e usarli per avere gli accessi privilegiati alle informazioni aziendali e alle loro applicazioni).

Questa tipologia di "lavoro agile", denominata smart working mette a dura prova la protezione dei dati personali, poiché non vi sono state ulteriori misure chiarificatrici, neanche da parte del nostro Garante, emanate per mitigare i rischi a cui essi sono così sottoposti e maggiormente esposti: si pensi ad esempio ai **frettolosi collegamenti da remoto effettuati** verso i server o i NAS del comune; si pensi a misure fittizie di "sicurezza fai da te"; si pensi all'**utilizzo dei propri device per svolgere l'attività lavorativa in totale assenza di misure tecniche di sicurezza**; si pensi alla mancanza di policy di sicurezza presenti solo all'interno delle mura scolastiche ed alla grandissima mole di dati personali messi a disposizione dei dipendenti all'esterno della scuola.

Requisiti minimi di sicurezza informatica su computer personali che devono accedere esclusivamente al software gestionale del comune via browser Web (no client/server):

1. assicurarsi di avere una buona connessione ad Internet (nel caso di connessioni scadenti si possono verificare corruzione dei dati);
2. controllare che il sistema operativo in uso sia aggiornato (Windows > 8.1, Mac > El Capitan);
3. Impostare una password di accesso al computer;
4. il pc deve essere ad uso esclusivo del dipendente (non utilizzato dai familiari);
5. utilizzare un Antivirus (non free) del tipo Internet Security (firewall integrato) e verificare che sia aggiornato;
6. Il computer deve avere installato solo i programmi necessari all'operatività aziendale (no programmi torrent, programmi non originali, programmi che possano registrare l'attività dell'utente, ecc.). A titolo indicativo e non esaustivo i programmi consentiti sono:

    a. Strumenti Produttività
        i. Open Office, Libre Office, Microsoft Office
    b. Browser Web
        i. Google Chrome, Firefox
    c. Utilità
        i. Acrobat Reader, 7zip
7. Mantenere riservate le password di accesso al gestionale e non memorizzarle all'interno del browser web
8. Eseguire sempre il log out quando si intende uscire dalla procedura gestionale

Requisiti aggiuntivi nel caso di accesso da parte del dipendente attraverso il proprio computer a materiale che si trova nel server/NAS del comune:

1. Instaurare una connessione VPN protetta tra il computer e la sede dell'Ente
    a. Una VPN (Virtual Private Network) consente di creare una rete privata virtuale che garantisce privacy, anonimato e sicurezza dei dati attraverso un canale di comunicazione riservato tra dispositivi dislocati nel territorio.
    b. Indipendentemente dalla tipologia VPN usata (accesso remoto/site-to-site) per instaurare una connessione tra un client ed il relativo server i passi che sono richiesti possono essere così riassunti:

        i. il client contatta il server;
        ii. il server notifica la propria presenza;
        iii. il client richiede al server di essere identificato;
        iv. il server verifica che il tentativo di connessione sia autorizzato previa autenticazione riuscita;
        v. il server risponde alla richiesta di autenticazione e autorizza la comunicazione con il client;
        vi. inizia la comunicazione tra le due entità.
2. Le credenziali per l'accesso alla VPN devono essere comunicate solo al dipendente.
3. Il comune deve tenere traccia degli accessi effettuati dai dipendenti attraverso un sistema di Log.

Utilizzo programmi di controllo remoto

Per le scuole che intendono avere la massima operativa e sicurezza senza la necessità di imporre prerequisiti ai computer personali dei dipendenti raccomando l'acquisto di software che permettano il controllo remoto della postazione di lavoro dell'ufficio (Supremo, TeamViewer, AnyDesk, ecc.).

Un software di controllo remoto è un programma grazie al quale, con una connessione internet e una password, si può accedere ad un altro computer operandovi come se si fosse in ufficio.

Vantaggi di questa soluzione:

1. Facile implementazione (basta installare un programma)
2. Il computer che si connette dall'esterno al comune è separato dal desktop remoto quindi non c'è promiscuità fra i 2 sistemi
3. La connessione è crittografata