Smart working P.A.: ricordiamo le raccomandazioni dell'AgID per la sicurezza

Scritto da Interdata Cuzzola | 25/03/2020

In tempi di Coronavirus lo smart working è tornato di grande attualità per i dipendenti pubblici.
E allora è utile ricordare la circolare 17 marzo 2017, n. 1, dell'Agenzia per l'Italia Digitale (AgID), che aveva già fornito 11 raccomandazioni per poter operare in sicurezza e che riportiamo di seguito a beneficio dei lettori:

1. seguire prioritariamente le policy e le raccomandazioni dettate dalla propria Amministrazione;
2. utilizzare i sistemi operativi per i quali attualmente è garantito il supporto;
3. effettuare costantemente gli aggiornamenti di sicurezza del sistema operativo;
4. assicurarsi che i software di protezione del sistema operativo (firewall, antivirus) siano abilitati e costantemente aggiornati;
5. assicurarsi che gli accessi al sistema operativo siano protetti da una password sicura e comunque conforme alle password policy emanate dalla propria Amministrazione;
6. non installare software proveniente da fonti/repository non ufficiali;
7. bloccare l'accesso al sistema e/o configurare la modalità di blocco automatico quando ci si allontana dalla postazione di lavoro;
8. non cliccare su link o allegati contenuti in email sospette;
9. utilizzare l'accesso a connessioni wi-fi adeguatamente protette;
10. collegarsi a dispositivi mobili (pen-drive, hdd-esterno) di cui si conosce la provenienza (nuovi, già utilizzati, forniti dalla propria Amministrazione);
11. effettua sempre il log-out dai servizi/portali utilizzati dopo aver concluso la sessione lavorativa.

Si tratta di raccomandazioni utili a contrastare eventuali attacchi informatici, attraverso comportamenti responsabili.