Smart Working nella PA: regole per i dipendenti

Direttive AgID per i dipendenti pubblici che lavorano in Smart Working: vademecum per la sicurezza informatica.

L'emergenza Coronavirus e i decreti-legge emanati nei giorni scorsi hanno portato a una maggiore diffusione dello **Smart Working** nella Pubblica Amministrazione, chiamata ad adottare il più possibile modalità di lavoro agile per tutelare la salute dei dipendenti e dei cittadini, limitando gli accessi agli uffici pubblici.

Smart work obbligatorio nella PA

4 Marzo 2020 Per aiutare i **dipendenti pubblici** a utilizzare al meglio e in sicurezza i propri dispositivi elettronici personali, come pc, smartphone e tablet, il Cert-PA di AgID ha realizzato un prezioso **vademecum** con undici semplici raccomandazioni elaborate sulla base delle minime di **sicurezza informatica** per le PA fissate dalla circolare n. 1/2017.

undici semplici raccomandazioni elaborate sulla base delle minime di **sicurezza informatica** per le PA fissate dalla circolare n. 1/2017.

L'obiettivo delle 11 regole è quello di supportare le PA e i lavoratori nel contrastare eventuali attacchi informatici con comportamenti responsabili:

- seguire le **policy** e le raccomandazioni dettate dall'amministrazione di riferimento;
- utilizzare i **sistemi operativi** per i quali attualmente è garantito il supporto;
- effettuare gli **aggiornamenti** di sicurezza del sistema operativo;
- assicurarsi che i software di **protezione del sistema operativo** (Firewall, Antivirus, ecc) siano abilitati e aggiornati;
- assicurarsi che gli accessi al sistema operativo siano protetti da**password sicura** e conforme alle policy emanate dalla PA;
- non **installare software** proveniente da fonti/repository non ufficiali;
- bloccare l'accesso al sistema e/o configurare il **blocco automatico** quando ci si allontana dalla postazione di lavoro;
- non cliccare su link o allegati contenuti in **email sospette**;
- utilizzare l'accesso a **connessioni Wi-Fi** adeguatamente protette
- collegarsi a dispositivi mobili (pen-drive, hdd-esterno, etc) di cui si conosce la provenienza;
- effettuare sempre il **log-out dai servizi/portali** utilizzati dopo che si ha concluso la sessione lavorativa.