Ministero dell'Istruzione

Dipartimento per le risorse umane, finanziarie e strumentali

Direzione Generale per i sistemi informativi e la statistica

Linee guida per l'utilizzo corretto delle nuove postazioni di lavoro

Gentile utente,

questa Direzione sta progressivamente procedendo alla sostituzione delle postazioni di lavoro di tutti gli utenti degli Uffici centrali e periferici del Ministero.

Le nuove postazioni sono di tipo portatile e garantiscono maggiori performance e sicurezza, essendo dotate di software e strumenti di lavoro aggiornati ai più recenti standard. Inoltre, grazie alle dimensioni e al peso molto contenuto, permettono agevolmente di lavorare in continuità sia in presenza che in smart working.

A tale proposito, si intende fornire alcune raccomandazioni per un utilizzo corretto.

Gestione delle Credenziali

Le password di accesso alla postazione di lavoro (relative alle utenze di tipo "MI" e "MIM") potranno essere modificate accedendo all'area riservata del portale istituzionale con la propria "utenza di portale" e seguendo il percorso: Profilo > Gestione profilo > Modifica password. Questa funzionalità SIDI è utilizzabile sia all'interno che all'esterno della rete ministeriale.

Si ricorda che "l'utenza di portale" ed è del tipo "nome.cognome" e coincide con l'utenza "MI" per il personale amministrativo, per il personale scolastico comandato-utilizzato o con l'utenza temporanea "MIT".

Si fa presente che la postazione di lavoro memorizza l'ultima password utilizzata per fare il login sulla rete ministeriale. Ciò comporta che, se la password viene modificata mentre non si è collegati a tale rete (ad esempio in smart working), sarà necessario accedere alla postazione con la vecchia password finché non ci si ricollegherà alla rete ministeriale.

La nuova password sarà invece valida anche fuori dalla rete ministeriale per effettuare l'accesso ad altri eventuali servizi disponibili on-line (SIDI, Office365, ecc.)

Pertanto, si rende necessario che:

- le password di accesso alla postazione di lavoro, alla posta e ai sistemi informativi siano sicure, complesse, non facilmente individuabili, diverse per servizi distinti e che, al momento della modifica, non siano differenziate solo da piccole variazioni (ad esempio cambio di un solo numero o di una sola lettera);
- la e-mail istituzionale non sia utilizzata per registrarsi in Internet a siti o servizi non riguardanti l'attività lavorativa;
- le password e le utenze con le quali si accede a siti o applicazioni web non vengano salvate nel browser di navigazione Internet.

Raccomandazioni sulla custodia della postazione

I dati presenti sulle nuove postazioni di lavoro sono sicuri in quanto memorizzati in forma crittografata.

I dati conservati in cloud (Microsoft OneDrive del MIUR) sono sicuri e gestiti secondo la normativa europea in materia di protezione dei dati personali.

Al fine di attuare ogni buona pratica a tutela della postazione di lavoro assegnata, si raccomanda di ancorarla, ove possibile, alla scrivania o ad altri mobili idonei utilizzando il cavo di sicurezza fornito. Si raccomanda, altresì, di non lasciare la postazione incustodita, chiudendo sempre a chiave la porta della propria stanza ed evitando che la stessa chiave sia facilmente accessibile ad eventuali malintenzionati.

Come di prassi, al termine dell'orario di servizio, la chiave della stanza potrà essere riposta nelle apposite bacheche, ove presenti, in modo da restare a disposizione dell'Ufficio.

In caso di utilizzo della postazione assegnata in smart working, dovrà essere adottata ogni cautela atta a limitare il rischio di furto, smarrimento, guasto o uso illecito. La postazione dovrà essere trasportata, conservata e utilizzata con cura.

Eventuali comportamenti non conformi potrebbero determinare l'irrogazione di sanzioni a carico del dipendente, in conformità a quanto previsto dal Codice di comportamento dell'Amministrazione.

Per le ragioni sopra evidenziate è fondamentale che eventuali furti siano immediatamente segnalati al proprio Dirigente, secondo le indicazioni riportate nell'area riservata del portale dei servizi > Computer Security Incident Response Team (CSIRT-MI) > Procedure Utente > Segnalazione di potenziale data breach.

Saranno in questo modo attivate una serie di contromisure che permetteranno anche di cancellare da remoto tutti i dati presenti nella postazione, limitando fortemente la possibilità di furto di dati riservati.

In caso di furto l'utente assegnatario dovrà presentare denuncia/querela alle competenti autorità entro 24 ore dall'evento. Copia della denuncia, insieme ad una breve relazione dell'accaduto, dovrà essere inviata dall'ufficio di appartenenza, tramite protocollo informatico, alla DGSIS (dgcasis@postacert.istruzione.it).

Conservazione dei dati (Backup)

Al fine di conservare le informazioni gestite ed utilizzate in ambito lavorativo è necessario che i relativi file siano periodicamente copiati come backup, utilizzando gli strumenti messi a disposizione dell'Amministrazione come Microsoft OneDrive.

Si raccomanda di limitare l'uso di supporti removibili quali chiavette usb e hard disk esterni, utilizzando gli strumenti messi a disposizione dell'Amministrazione. Ove fosse indispensabile utilizzare i supporti removibili, si raccomanda di farlo con molta cautela, verificando preventivamente l'assenza di virus mediante l'apposito software fornito.

Questa accortezza, in aggiunta alle indicazioni operative da seguire in caso di furto o smarrimento, permetterà di conservare sempre una copia dei documenti di lavoro in ogni circostanza.

Nell'utilizzo dello strumento specifico Microsoft OneDrive si raccomanda di fare attenzione alle eventuali condivisioni dei file, assicurandosi di selezionare specifici colleghi dell'Amministrazione e attribuendo i corretti permessi di lettura/scrittura.

Corretto utilizzo della Posta elettronica

Allo scopo di impedire il verificarsi di eventuali incidenti di sicurezza, derivanti dall'uso non corretto della posta elettronica istituzionale, si forniscono le seguenti raccomandazioni:

- non aprire file non attesi, dalla dubbia provenienza o che giungano da caselle di posta non note;
- non tentare di installare autonomamente software sulla propria postazione, soprattutto se a seguito di inviti via e-mail che presentino link di accesso ad altre pagine o che suggeriscano l'esecuzione di file.
- non dare seguito alle richieste di e-mail sospette;
- nel caso in cui la richiesta provenga da parte del personale tecnico della nostra Amministrazione, verificarne l'autenticità, valutando che il testo del messaggio presenti una grammatica e una sintassi corretta, che eventuali link contenuti nell'e-mail puntino a siti conosciuti e che il mittente sia noto o corretto.

Si ringrazia per la collaborazione

IL DIRETTORE GENERALE

Gianna Barbieri

Firmato digitalmente da
BARBIERI GIANNA
C=IT
O=MINISTERO
DELL'ISTRUZIONE