Ministero dell'istruzione

Dipartimento per le risorse umane, finanziarie e strumentali

Direzione Generale per i sistemi informativi e la statistica

POLITICHE PER LA SICUREZZA DELLE INFORMAZIONI

PER GLI UTENTI DEL SISTEMA INFORMATIVO

DELL'ISTRUZIONE

PER IL PERSONALE ATA

SOMMARIO

Fare clic o toccare qui per immettere il testo.

1 Riferimenti generali

1.1 Traccia delle versioni

numero versione	data ultima modifica
v. 2.1	20/12/2021

1.2 Scopo della politica

Questo documento fornisce al personale utente del *Sistema Informativo del Ministero dell'Istruzione* una panoramica sulle responsabilità loro spettanti in merito alla gestione ed allo sviluppo della sicurezza delle informazioni, allo scopo di accrescere la cultura della sicurezza e le politiche di utilizzo dei sistemi informativi che il personale utilizza per connettersi alle infrastrutture del Ministero dell'Istruzione. Tramite le presenti politiche il Ministero dell'Istruzione intende agevolare e diffondere la conoscenza delle singole attività che il lettore è responsabilizzato a seguire per garantire l'innalzamento del livello di sicurezza della struttura.

Il termine "sicurezza" si riferisce a tre aspetti distinti:

- **Riservatezza**: Prevenzione contro l'accesso non autorizzato alle informazioni e conformità dell'utilizzo alle linee guida del Garante per il trattamento dei dati personali;
- **Integrità**: Le informazioni non devono risultare alterabili da incidenti o abusi;
- **Disponibilità**: Il sistema deve essere protetto da interruzioni impreviste.

Il raggiungimento di questi obiettivi richiede non solo l'utilizzo di appropriati strumenti tecnologici, ma anche opportuni meccanismi organizzativi; misure esclusivamente di natura tecnica, per quanto sofisticate, potrebbero non risultare efficienti laddove usate impropriamente.

1.3 Destinatari

La presente politica si applica a tutto il personale ATA del Ministero dell'Istruzione.

2 Guida alla lettura del documento

Questo documento contiene le politiche per la sicurezza delle informazioni del Sistema Informativo dell'Istruzione. È possibile leggere la politica per intero o utilizzare il sommario all'inizio del documento per accedere ai singoli capitoli e/o sezioni interessate.

Nel cap. 1 viene definito lo scopo generale della politica e gli utenti destinatari della presente politica.

Il cap. 3 fornisce una panoramica generale sui sistemi informativi e la sicurezza informatica. Rende note, inoltre, le responsabilità dell'utente e dell'Amministrazione in materia di sicurezza informatica.

Nel cap. 4 viene delineata la regolamentazione dell'utilizzo della posta elettronica, con le relative indicazioni per l'attivazione del servizio e gestione delle password, con particolare riguardo agli utilizzi consentiti e alle limitazioni del servizio.

Nel cap. 5 sono presenti le linee guida per la gestione dei dispositivi personali (pc, smartphone e tablet), in particolar modo per rendere attuabile in modo sicuro lo smart-working.

Il cap. 6 informa gli utenti sulle modalità di accesso ai servizi dell'amministrazione.

Il cap. 7 informa gli utenti sul trattamento dei dati personali, esteso a tutte le casistiche di cui sopra.

I cap. 8 e 9 forniscono una migliore lettura del documento, grazie ad un glossario di definizioni e i richiami di tutti i riferimenti normativi citati nella presente politica.

3 Informativa sulla sicurezza del SGSI

La presente informativa si pone l'obiettivo di:

- fornire una sintetica disamina sulla classificazione di dati ed informazioni che il personale dipendente potrebbe trovarsi a gestire;

- prevenire gli incidenti della sicurezza delle informazioni e minimizzarne gli impatti;
- assicurare la continuità dei servizi forniti dal Sistema Informativo dell'Istruzione;
- minimizzare i danni in caso di incidente e/o di avaria e massimizzare il rendimento del capitale investito e le opportunità di miglioramento in materia di sicurezza delle informazioni;
- proteggere i dati e garantire la conformità delle misure di sicurezza adottate e dell'organizzazione del MI a tutte le regole di natura normativa esistenti, con particolare riguardo alla protezione delle informazioni di natura personale.

Sulla base di quanto condiviso, si pone la necessità di definire i principi per la protezione dei beni informativi del Sistema Informativo dell'Istruzione da tutte le minacce che possano pregiudicare:

- l'integrità delle informazioni,
- la disponibilità del servizio e delle informazioni,
- la riservatezza delle informazioni dalle minacce interne e/o esterne, deliberate e/o accidentali, ma comunque riconducibili ai beni informativi del MI. L'Amministrazione si impegna altresì a fornire linee guida, consulenza e risorse applicative e/o tecnologiche alle istituzioni scolastiche, Enti Vigilati e siti Speciali, affinché, nella loro autonomia e responsabilità, possano provvedere alla messa in sicurezza del proprio patrimonio informativo.

Viene predisposto un modello organizzativo destinato:

- all'amministrazione in maniera organica della sicurezza del sistema informativo dell'istruzione;
- al supporto coordinato ai diversi Uffici dell'Amministrazione ai quali è demandata la responsabilità della gestione di fornitori esterni (outsourcer) i cui servizi incidono sull'amministrazione del sistema informativo dell'istruzione;
- ad aggiornare le diverse Policy predisposte dall'Amministrazione per disciplinare termini e modalità di utilizzo degli strumenti elettronici all'interno dell'Amministrazione.

Con riferimento a quanto previsto dal D.Lgs. 101/2018 e dal Regolamento UE 679/2016 (GDPR), si ribadiscono in particolare le disposizioni che stabiliscono che i dati personali devono essere protetti

adeguatamente sia al fine di evitare accessi non autorizzati e trattamenti illeciti, sia per ridurre al minimo, mediante l'adozione di adeguate misure, i rischi di distruzione e perdita dei dati e delle informazioni.

È politica del MI:

- garantire la corretta formazione, raccolta e conservazione dei dati;
- garantire la continuità operativa dei sistemi informativi di cui l'Amministrazione si avvale per lo svolgimento delle proprie funzioni istituzionali;
- prevenire l'uso improprio degli impianti e dei sistemi di elaborazione delle informazioni;
- controllare e regolamentare l'accesso al patrimonio informativo, effettuato dai fornitori del MI, nell'ambito delle attività previste dal contratto di gestione in outsourcing o nell'ambito di ogni ulteriore rapporto contrattuale in essere con la DGSI;
- garantire la conformità alle politiche per la sicurezza, assicurandone la diffusione dei principi presso tutto il personale dell'amministrazione e il personale esterno che si trovi ad interagire con il sistema informativo;
- garantire la corretta elaborazione e la protezione delle informazioni aziendali;
- garantire la disponibilità delle informazioni, degli impianti e dei sistemi di elaborazione delle informazioni e la conformità del trattamento delle informazioni contenenti dati personali;
- produrre, mantenere e sottoporre a prove periodiche, con il supporto dei Fornitori, i piani per la continuità dei servizi informatici erogati nell'ambito del contratto di outsourcing;
- assicurarsi che siano poste in atto tutte le necessarie azioni al fine di ridurre i rischi connessi alle seguenti minacce:
    - Infrazioni della sicurezza dovute a carenze organizzative,
    - Incidenti e avarie dei sistemi di elaborazione,
    - Uso non autorizzato o improprio di impianti, sistemi di elaborazione delle

informazioni, utilità di sistema o applicazioni, rimozione non autorizzata di oggetti,

- Accesso non autorizzato a informazioni o sistemi
- Codice malevolo, virus, worm, trojan, phishing
- Comportamenti scorretti o non conformi dell'utente,
- Ogni altro tipo di attacco proveniente dalla rete internet;

- rendere disponibile a tutto il personale del MI, ed in particolare agli utenti del Sistema Informativo dell'Istruzione, adeguata formazione sulla sicurezza delle informazioni e sulle procedure messe in atto per la gestione della stessa;
- raccogliere segnalazioni e formalizzare rapporti su tutte le infrazioni della sicurezza e condurre indagini coordinate dal CSIRT del MI, in collaborazione con il Responsabile della Sicurezza del Fornitore dei Servizi di gestione di tale Sistema;
- realizzare e mantenere aggiornate in conformità alle esigenze del MI, con il coinvolgimento del Fornitore, procedure a sostegno della Politica, che includano almeno:
  - classificazione e controllo dei beni,
  - protezione fisica delle risorse,
  - protezione logica delle informazioni,
  - gestione dei supporti rimovibili,
  - back-up delle informazioni,
  - gestione degli incidenti e dei malfunzionamenti inerenti la sicurezza,
  - controlli antivirus e antispamming,
  - gestione degli scambi di informazioni, regolamentazione dell'accesso al sistema informativo del MI da parte di enti esterni,
  - utilizzo della crittografia e della firma digitale laddove appropriato,

- sicurezza dei sistemi di automazione d'ufficio,
- gestione, monitoraggio e controllo degli accessi degli utenti ai sistemi e alla rete,
- sviluppo e manutenzione dei sistemi,
- garanzia della continuità dei servizi, nel rispetto dei livelli di servizio contrattuali,
- verifica periodica di efficacia e di validità nel tempo delle contromisure adottate, mediante la definizione di opportune metriche e l'implementazione di sistemi di monitoraggio e controllo.

Il Responsabile per la Sicurezza delle Informazioni del Sistema Informativo dell'Istruzione ha la diretta responsabilità per l'attuazione, la verifica e il miglioramento della presente Politica, in relazione all'uso del Sistema Informativo dell'Istruzione e dei servizi a questo collegati.

Tutti gli utenti del Sistema Informativo dell'Istruzione e il personale del Fornitore dei servizi di sviluppo e gestione dello stesso, sono responsabili dell'attuazione della presente Politica.

3.1 Classificazione di dati e informazioni

Dati e **informazioni** sono elementi distinti ma profondamente correlati.

I **dati** fanno tipicamente riferimento a elementi grezzi o non preventivamente elaborati e, in tal senso, costituiscono la forma di base che, una volta sottoposti ad elaborazione ed analisi i dati si traducono in informazioni.

In termini generali, un dato può risultare rappresentato attraverso un numero, un segnale o un testo; si tratta di contenuti certamente caratterizzati da un valore proprio ma che, tuttavia, a seconda del contesto in cui siano inseriti possono assumere significati e fornire **informazioni** differenti. Il numero 10, ad esempio, può rappresentare un voto eccellente se assegnato ad uno studente delle scuole superiori ma un pessimo voto per uno studente universitario, una temperatura troppo bassa per uscire in maniche di camicia, ma troppo alta per conservare correttamente alimenti.

L'**informazione** è, di converso, "*una forma di conoscenza acquisita, trasmessa o condivisa attraverso dati associati ad uno specifico fatto o circostanza*". L'informazione è pertanto una sequenza di simboli

che può essere interpretata come un messaggio utile a fornire conoscenze o dettagli in relazione a un determinato tema.

Ciò sinteticamente premesso, il Ministero dell'Istruzione ha adottato un processo di classificazione, etichettatura e gestione di dati ed informazioni che è funzionale a garantire:

- la corretta classificazione, etichettatura e gestione di tutte le informazioni acquisite, conferite al Ministero dell'Istruzione e alle sue strutture organizzative o da esse stesse generate, trasferite o condivise, indipendentemente dal supporto fisico o immateriale;
- che le risorse, preventivamente etichettate in relazione al loro specifico contenuto secondo la classificazione di seguito dettagliata, possano:
    - ricevere un livello adeguato di protezione,
    - esser gestite nel loro utilizzo in modo appropriato.

Gli standard adottati si applicano all'intera gamma di dati ed informazioni, ivi incluse quelle conferite da terzi o di propria pertinenza e fanno riferimento alle seguenti risorse:

- **Risorse fisiche**: fascicoli e documenti, archivi fisici sia centralizzati che distribuiti, apparecchiature informatiche, apparecchiature di comunicazione, dispositivi di sicurezza, supporti magnetici, altre apparecchiature tecniche;
- **Risorse software**: software applicativo, strumenti di sviluppo e utilità;
- **Risorse informative**: database e file di dati, documentazione di sistema, manuali utente, materiale di formazione, procedure operative o di supporto, informazioni archiviate

Più nel dettaglio la classificazione dei dati e delle informazioni che gli utenti del Sistema Informativo, in base alla propria area di competenza, potrebbero trovarsi a gestire e/o elaborare ricade all'interno delle seguenti tipologie:

- **Riservata**: rientrano nel segmento tutti quei dati e informazioni i cui contenuti non possano essere divulgati a terzi in quanto, laddove diffusi al di fuori del perimetro di condivisione

preliminarmente definito, potrebbero generare danni di immagine, di reputazione o economici o generare indesiderabili effetti anche su terzi

- **Confidenziale**: rispetto al perimetro di una specifica struttura organizzativa, ricadono nel segmento tutti i dati e le informazioni, anche riservati, idonei a poter esser condivisi anche all'esterno del perimetro purché a solo beneficio di alcuni soggetti preliminarmente identificati e secondo determinate regole. La salvaguardia di tali dati e informazioni può essere disciplinata, ad esempio, attraverso un accordo di non divulgabilità in cui siano specificati i limiti di diffusione e di utilizzo di dati e informazioni conferiti in via confidenziale a un soggetto esterno
- **Personale**: qualsiasi dato o informazione riguardante una persona fisica identificata o identificabile e sottoposta a protezione ai sensi di quanto previsto dal Regolamento UE 679/2016 (GDPR) anche acquisita, elaborata o generata nel corso delle attività istituzionali o di erogazione dei servizi in favore dei propri utenti,
    - sia di titolarità del Ministero dell'Istruzione stesso o di strutture organizzative ad esso riconducibili,
    - sia conferita o trasferita al Ministero dell'Istruzione stesso o a sue strutture organizzative per il tramite di Istituti scolastici, famiglie, altre Amministrazioni, enti ed altri soggetti fisici, giuridici o economici anche in qualità di Responsabile al trattamento dei dati personali.
- **Particolare**: nel segmento afferiscono le categorie di dati e di informazioni di natura Personale che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici o biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona il cui trattamento è disciplinato dal Regolamento UE 679/2016 (GDPR).
- **Interna**: informazioni la cui diffusione all'interno di ciascuna struttura organizzativa del Ministero dell'Istruzione non causi impatti sull'erogazione dei servizi in favore della propria specifica utenza ma che, in quanto riguardanti processi e flussi interni e riferite a elementi non

di pubblico dominio (anche temporaneamente), non si ritiene debbano essere condivise con soggetti al di fuori del perimetro organizzativo.

- **Pubblica**: sono tutti i dati e le informazioni, sia generate che divenute nel tempo di dominio pubblico e la cui diffusione non generi impatti sull'erogazione dei servizi da parte del Ministero dell'Istruzione e delle sue strutture organizzative in favore dei propri utenti.

Rispetto alla premessa classificazione si sottolinea che:

- ciascun dato o informazione rientrante nelle tipologie **Personale e Particolare** sia soggetta alle prescrizioni del Regolamento UE 679/2016 (GDPR);
- elementi di protezione aggiuntiva debbano essere comunque garantiti al fine di preservare dati ed informazioni dalla diffusione al di fuori del perimetro di loro stretta pertinenza.

3.2 Responsabilità per la sicurezza

La fruizione dei servizi informatici del MI si basa su norme e procedure operative che garantiscono un adeguato livello di sicurezza nel rispetto delle politiche dell'Amministrazione e delle leggi vigenti.

Ogni utente ha la responsabilità di osservare le disposizioni emanate dall'Amministrazione, al fine di evitare violazioni delle procedure di sicurezza o un degrado del livello dei servizi forniti.

A tal proposito si sottolinea che la responsabilità delle azioni compiute nell'esercizio delle proprie mansioni è del singolo. In particolare, il personale è responsabile del corretto utilizzo degli strumenti d'identificazione personale, della segretezza dei propri codici d'accesso, delle operazioni compiute tramite i sistemi informatici messi a disposizione.

È compito di tutto il personale vigilare sull'osservanza delle misure di sicurezza, di segnalare al proprio Referente Informatico possibili problemi relativi alla sicurezza e all'erogazione dei servizi, di porre in atto le misure ed i comportamenti più opportuni al fine di raggiungere e mantenere il livello di sicurezza e di servizio prefissato, in rapporto alle proprie mansioni e capacità.

3.3 Mappatura dei ruoli

È titolare e responsabile dell'attuazione della presente politica il Direttore Generale della DG SIS.

Gli utenti hanno la responsabilità di rivolgersi per ogni anomalia rilevata e per segnalare problemi inerenti la sicurezza al proprio Referente Informatico, il quale è demandato ad interloquire con lo CSIRT MI per anomalie rilevate in ambito di sicurezza e sarà tenuto ad informare il dirigente della struttura in caso di possibile violazione dei dati soggetti a protezione (Data Breach).

4 Regole per l'utilizzo della posta elettronica

L'Amministrazione incoraggia l'uso della posta elettronica per scambiare informazioni, migliorare le comunicazioni, scambiare idee e per rendere più efficaci ed efficienti i processi di lavoro a supporto della missione istituzionale dell'Amministrazione.

In particolare, l'Amministrazione, anche sulla base delle direttive del Governo tese a promuovere la crescita delle comunicazioni in formato digitale e l'abbattimento di quelle cartacee, considera la posta elettronica uno strumento fondamentale, che viene messo a disposizione di tutti coloro che ne abbiano diritto.

Si fa presente che la presente politica si applica sia ai contenuti dei messaggi di posta elettronica, sia alle informazioni transazionali (header dei messaggi, indirizzi di posta, dati dei destinatari e dei mittenti) relative a tali messaggi.

4.1 Attivazione del servizio

Il servizio di posta elettronica è attivato, per ogni utente che ne abbia diritto ed è gratuito. Il Ministero fornisce all'Utente del servizio un Codice Utente ed una Password modificabile. L'accesso al Servizio è consentito solo mediante tali identificativi.

Il servizio rimarrà attivo per tutto il periodo in cui rimarrà valido il rapporto con l'Amministrazione. Al trascorrere di 6 mesi dal termine del rapporto con l'Amministrazione, il servizio sarà disattivato senza necessità di assenso da parte dell'utente e l'account di posta elettronica verrà cancellato.

Sarà cura dell'Utente del servizio provvedere al salvataggio dei dati e dei messaggi prima della disattivazione del servizio, da effettuarsi esclusivamente per fini lavorativi. Non è prevista alcuna forma di indennizzo per il venir meno del servizio.

4.2 Usi consentiti e limitazioni

Le finalità di utilizzo della posta elettronica sono legate all'attività lavorativa svolta o per finalità istituzionali. È proibito l'utilizzo del servizio per fini privati o personali.

L'utente è edotto del fatto che l'Amministrazione considererà, ai fini di eventuali ispezioni, tutti i messaggi di posta elettronica da lui gestiti come strettamente afferenti all'uso del servizio per scopi di lavoro. Si ricorda, comunque, che per gli usi personali è possibile e consigliato dotarsi di una casella di posta elettronica alternativa, ottenibile gratuitamente presso molti fornitori esterni, e liberamente consultabile via internet.

L'uso del servizio di posta elettronica dell'Amministrazione è soggetto alle seguenti condizioni:

- è fatto divieto di inviare intenzionalmente o involontariamente dalla casella di posta elettronica dell'Amministrazione messaggi di posta indesiderata, lettere a catena o qualsiasi altro tipo di distribuzione massiva non autorizzata di posta indesiderata; ciò potrebbe avere impatti sulla reputazione di tutto il servizio di posta elettronica e influire sul recapito della posta elettronica degli altri utenti del servizio erogato dall'Amministrazione;
- non è possibile utilizzare la casella di posta per attività commerciali o per attività politiche o per trasmettere materiale in violazione dei diritti d'autore;
- è vietata la creazione e utilizzo di un indirizzo e-mail falso o alias al fine di impersonare un'altra identità o inviare comunicazioni fraudolente;
- è vietato a tutti gli Utenti l'utilizzo del servizio di posta elettronica di inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione

dell'Amministrazione.

- È inoltre vietato l'uso del servizio di posta elettronica a scopi di profitto personale e per attività illegali e la fornitura (gratuita o a pagamento) a persone fisiche o giuridiche di qualsiasi lista o elenco degli Utenti del Servizio. Chiunque riceva comunicazioni della natura sopra indicata dovrà segnalarlo alla Direzione Generale per i sistemi informativi e la statistica, avvalendosi dei servizi di assistenza accessibili attraverso il canale del Service Desk del Ministero. È proibito, inoltre, fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi e-mail che facciano richiesta di questo tipo di informazioni;
- non è consentito utilizzare l'indirizzo di posta elettronica per la registrazione a siti web e a portali visitati per scopi personali. Nel caso in cui sia necessario registrarsi ad un portale per scopi lavorativi, si ricorda di non utilizzare password già adottate in qualsiasi ambito.
- Non è consentito impostare inoltri automatici di e-mail verso domini esterni non afferenti al Ministero dell'Istruzione.

Nell'ipotesi in cui la posta elettronica debba essere utilizzata per la trasmissione di categorie particolari di dati, si raccomanda di prestare attenzione a che:

- il destinatario sia effettivamente competente e autorizzato a ricevere i dati inviati;
- l'indirizzo del destinatario sia stato correttamente digitato;
- l'oggetto del messaggio non contenga direttamente il riferimento a stati, fatti o qualità idonei a rivelare dati di natura sensibile;
- nel corpo del messaggio sia presente un'intestazione standardizzata in cui si avverta della confidenzialità/riservatezza del messaggio.

4.3 Utilizzo in caso di assenza

In caso di assenza programmata (ad esempio, per ferie o attività di lavoro fuori sede):

- l'Utente è invitato ad avvalersi delle specifiche funzionalità di sistema che consentano di inviare

automaticamente messaggi di risposta contenenti i riferimenti di contatto di un altro soggetto o altre utili modalità di contatto dell'Amministrazione. Quanto sopra allo scopo di assicurare la continuità operativa e senza dover vincolare l'Amministrazione o suoi Utenti a consultare caselle di posta nei momenti in cui l'utente non sia presente.

4.4 Rischi derivanti dall'utilizzo della posta elettronica

La posta elettronica è uno strumento molto facile da utilizzare e utile a garantire una rapida consegna dei messaggi. Nonostante la sua semplicità, è bene tenere a mente alcuni aspetti legati al suo funzionamento e che possono presentare dei rischi in termini di sicurezza sia per l'Utente che per il Ministero.

I messaggi di posta elettronica spediti ad una persona possono essere facilmente inoltrati ad altri destinatari. Al riguardo il Ministero non può proteggere gli utenti da fatti come quelli descritti che esulano dalle proprie possibilità e compiti. Gli utenti, pertanto, devono esercitare la massima cautela nell'uso della posta elettronica per comunicare informazioni riservate o categorie particolari di dati personali (v. art. 9 GDPR).

Non c'è garanzia, a meno di utilizzare sistemi di posta certificata, che i messaggi ricevuti provengano effettivamente dal mittente previsto; ciò in quanto è piuttosto semplice per i mittenti mascherare la propria identità, anche se ciò costituisce, tra le altre cose, una violazione della presente politica. Inoltre, i messaggi di posta che arrivano come "inoltro" di precedenti messaggi, potrebbero essere stati modificati rispetto all'originale. Pertanto, in caso di dubbi, chi riceva un messaggio di posta elettronica dovrebbe verificare con il mittente l'autenticità delle informazioni ricevute.

4.4.1 Altri consigli pratici

- Allegati: gli antivirus sono in grado di identificare ed eliminare i principali virus nascosti negli allegati; tuttavia, è sempre possibile che qualche virus, specie di più recente generazione, non venga intercettato. Si consiglia quindi non aprire e-mail con allegati sospetti specialmente se non se ne conosca la provenienza. Particolare attenzione deve essere rivolta anche a messaggi provenienti da indirizzi conosciuti, in quanto molti virus sono progettati per veicolarsi in rete

tramite gli indirizzi contenuti nella rubrica dell'utente.

- Link (collegamenti): prestare attenzione ai link contenuti nelle e-mail e cliccarli solo dopo aver controllato l'indirizzo di destinazione posizionando il cursore del mouse sulla stringa evidenziata: il collegamento può condurre a siti malevoli come portali replica di altri; si ricordi infatti che l'indirizzo cliccabile può essere diverso dall'indirizzo effettivo (provate qui: www.sembrounacosa.it); se si sta usando un tablet o smartphone, basta tenere premuto sul link per leggere la destinazione effettiva; prestare attenzione in particolare alla parte finale dell'indirizzo URL, ad esempio http://www.miur.gov.aka.it/ fa parte del dominio aka.it e non di quello gov.it.
- È buona norma evitare di rispondere alle e-mail rinviando allegati non necessari.

4.4.2 Restrizioni all'uso del servizio

Gli utenti del servizio di posta elettronica sono tenuti ad usarlo in modo responsabile, cioè, rispettando le leggi, la presente e altre politiche e procedure del Ministero e secondo normali standard di cortesia, correttezza, buona fede e diligenza professionale. L'accesso ai servizi di posta elettronica dall'Amministrazione può essere totalmente o parzialmente limitato dall'Amministrazione stessa, senza necessità di assenso da parte dell'utente e anche senza preavviso:

- quando richiesto dalla legge e in conformità ad essa;
- in caso di comprovati motivi che facciano ritenere la violazione della presente politica o delle disposizioni di legge vigenti;
- al venir meno delle condizioni in base alle quali si ha facoltà di utilizzare il servizio (ad es. cessazione per qualsiasi motivo del rapporto di lavoro con l'Amministrazione);
- in casi eccezionali, quando richiesto per esigenze operative critiche e improcrastinabili.

5 Linee guida sulla gestione dei dispositivi personali (smart-working)

In considerazione dei recenti DPCM e dell'articolo 14 della legge 124/2015, il MI adotta misure organizzative volte all'attuazione e al regolamento dello smart working e fornisce in questo capitolo le linee guida per una gestione sicura del telelavoro. In conseguenza dell'emergenza COVID-19 e di quanto sopra citato, fermo restando l'applicazione delle regole in ambito di Postazioni di Lavoro, lo smart working può essere svolto utilizzando strumenti non necessariamente forniti dal MI. Pertanto, al fine di incrementare il livello di sicurezza delle postazioni individuali remote, è fortemente consigliato agli utenti di dotarsi di quante più possibili fra le misure di sicurezza descritte nel presente documento, seguendo le presenti linee guida con diligenza e rigore, consapevoli delle conseguenze che possono derivare al loro stesso ambiente di lavoro domestico e ai sistemi del ministero.

Le presenti linee guida sono utili all'innalzamento della sicurezza oltre che alla sensibilizzazione sul tema; questi semplici accorgimenti possono contribuire ad aumentare sensibilmente lo stato di sicurezza delle postazioni di lavoro come delle singole postazioni private, contribuendo dunque a proteggere i dati personali, le informazioni sensibili e le connessioni dei dispositivi.

5.1 Connessione e accesso a internet

La connessione alla rete internet è il maggior vettore di attacchi informatici; è quindi buona norma provvedere alla protezione della rete domestica, avvalendosi di password complesse per la connessione ad Internet. Nel caso si disponga di una rete Wi-Fi, si consiglia di utilizzare una password complessa e di verificare che il protocollo in uso sia di tipo WPA2, poiché garantisce una maggior sicurezza a livello di cifratura e non consente a malintenzionati di venire a conoscenza della password e di accedere alla rete domestica.

Rimane quindi vivamente sconsigliata la connessione ad Internet tramite reti pubbliche.

In ogni caso, è sempre fortemente consigliato, all'atto della connessione ad Internet verificare il livello di sicurezza della connessione. Esistono tool gratuiti online con cui è possibile farlo. Uno di questi, a

scopo illustrativo, è "CheckME Joshua", il quale verifica la sicurezza della rete, del sistema operativo e del browser indicando, qualora possibile, le azioni da intraprendere per navigare in rete in modo sicuro *(v. 8.2.11)*.

Si consiglia inoltre di evitare di iscriversi a siti internet non riconducibili alla sfera lavorativa utilizzando la casella di posta istituzionale; tali siti potrebbero infatti essere poco sicuri nella protezione dei dati personali, con eventuali ripercussioni in violazioni all'interno della propria operatività lavorativa. A tal riguardo, si ricorda che non bisogna seguire in ogni caso la pratica del *password reuse*. È proibito fornire le proprie credenziali di accesso a sistemi o procedure, così come rispondere a messaggi che facciano richiesta di questo tipo di informazioni. Inoltre, evitare l'uso dei social network, o altre applicazioni social facilmente hackerabili con l'utenza adoperata per le attività lavorative.

5.2 Postazioni fisse e notebook

5.2.1 Sistema Operativo

Prima di impiegare dispositivi personali in ambito lavorativo è sempre bene verificare il sistema operativo dello strumento di utilizzo. Il sistema operativo in questione dovrebbe essere aggiornato con le ultime novità in ambito di sicurezza e non rientrare nelle sfere *End-of-life* o *End-of-support*.

Nel caso di un sistema operativo Windows, è possibile verificare lo stato degli aggiornamenti di sicurezza tramite i seguenti passaggi: selezionare il pulsante *Start*, andare su *Impostazioni*, quindi su *Aggiornamento e Sicurezza* e fare clic su *Windows Update*.

Nel caso di un sistema operativo MAC, è possibile verificare lo stato degli aggiornamenti di sicurezza tramite i seguenti passaggi: nel *menù Apple*, scegliere *Preferenze di Sistema*, quindi fare click su *Aggiornamento Software*.

Qualora il sistema operativo non risultasse aggiornato, è buona norma procedere ad installare gli aggiornamenti prima di iniziare ad utilizzare la postazione.

5.2.2 Software

Per il corretto svolgimento delle attività lavorative, potrebbe essere richiesto l'utilizzo di software di

uso comune. È raccomandabile utilizzare sempre software leciti e aggiornati, pertanto è opportuno verificare lo stato di aggiornamento di tali software ed adeguarlo, ove necessario, all'ultima versione rilasciata. È opportuno prestare particolare attenzione al livello di aggiornamento del browser utilizzato per navigare in internet, in quanto è uno dei più comuni punti d'accesso per la violazione dei computer. È buona norma, in generale, scaricare e installare solamente software provenienti da fonti affidabili e accreditate.

Con l'occasione si ricorda agli utenti che l'utilizzo di software "pirata", ossia senza licenza o la cui licenza viene bypassata tramite crack, è illegale anche in ambito privato e può portare a sanzioni amministrative in base alla L. 248/2000 sul diritto di autore.

5.2.3 Antivirus

Un antivirus è un software finalizzato a prevenire, rilevare ed eventualmente rendere inoffensivi codici dannosi e malware, è pertanto in grado di segnalare tentativi di compromissione o software malevoli presenti all'interno del computer. Di norma tutti gli antivirus effettuano scansioni periodiche, tuttavia, prima di procedere con l'utilizzo del proprio dispositivo in ambito lavorativo, è buona norma richiedere all'antivirus una scansione veloce del computer.

Tutti i possessori di Windows avranno integrato il sistema "Sicurezza di Windows" che avvertirà l'utente di ogni anomalia riscontrata sulla postazione di lavoro.

L'antivirus, più di tutti gli altri software, dovrebbe essere costantemente aggiornato. Solo in questo modo, infatti, potrà proteggere l'utente dalle più recenti minacce informatiche.

Nel caso l'utente non disponga di un software antivirus già precedentemente installato sul proprio dispositivo, si rende noto che in rete sono presenti prodotti molto validi e totalmente gratuiti, che possono essere scaricati direttamente da internet e possono proteggere il computer dai più comuni attacchi informatici *(v. 8.2.11).*

5.2.4 Ambienti separati, password e blocco schermo

È sempre buona norma che il dispositivo sia protetto da password e che lo schermo sia impostato sul blocco automatico dopo un lasso di tempo di inattività (preferibilmente dopo un massimo di 10 minuti)

in modo che la postazione non possa essere utilizzata da persone non autorizzate.

A tal proposito, al fine di proteggere i dati e i file utilizzati a scopo lavorativo, è preferibile creare un'apposita utenza, in modo che altri eventuali utilizzatori del computer non possano accedere a dati sensibili e/o modificare file in uso. Si consiglia pertanto di creare un utente separato, da usare solo durante l'attività lavorativa e che abbia una password diversa da quella degli altri fruitori del computer.

5.2.5 Blocco Pop-Up

Molte minacce del mondo informatico provengono da pop-up pubblicitari che possono attivarsi automaticamente durante la normale navigazione in internet. Per prevenire questa problematica è utile installare un'estensione nel browser che blocchi le pubblicità. In questo modo, oltre ad aggiungere un livello di protezione del dispositivo, molti siti internet saranno più facilmente fruibili e la navigazione non verrà interrotta.

L'estensione più nota e sicura in quest'ambito si chiama "Adblock" (valida per Internet Explorer, Chrome, Firefox, Safari e Opera), è gratuitamente scaricabile da internet *(v. 8.2.11)*. Inoltre, si rende noto che è possibile abilitare e disabilitare questa estensione a piacimento con un semplice click del mouse; pertanto, l'estensione non è invasiva e non procura in alcun modo il rallentamento delle prestazioni della postazione utilizzata.

5.2.6 Gestione dei documenti

I documenti utilizzati durante l'espletamento delle proprie mansioni lavorative devono essere protetti da eventuali danni o manomissioni. Per questo motivo è consigliabile non salvare i file in locale sul dispositivo ma avvalersi dei sistemi cloud (o Onedrive) forniti dal MI, in modo che i documenti utilizzati/prodotti durante l'attività in smart working non possano essere raggiunti da terze parti, possano essere facilmente utilizzati nella loro ultima versione all'eventuale rientro in sede e non siano soggetti a perdite di dati in caso di guasto del computer. Eseguire con regolarità il backup periodico dei dati elaborati sul proprio PC nell'ambito della sfera lavorativa in modo da avere sempre un backup aggiornato dal quale eventualmente reperire i file.

Spesso lo smarrimento o il furto dei dispositivi può comportare il rischio che soggetti non autorizzati

possano accedere ai device e quindi a dati personali o aziendali; per prevenire il danno di tali situazioni si possono adottare delle soluzioni di cifratura ai vari dispositivi utilizzando software presenti sul mercato.

5.2.7 Gestione della posta elettronica

Allo scopo di ridurre i rischi di sicurezza correlati ai client installati su PC potenzialmente non protetti o compromessi, si raccomanda caldamente di utilizzare la versione webmail per accedere ed utilizzare la posta elettronica. In questo modo software terzi non potranno venire a conoscenza delle credenziali utilizzate per accedere al servizio.

5.2.8 Utilizzo VPN

In caso si rendesse necessario, il MI provvede a fornire le credenziali per una VPN che concede l'accesso ad alcune applicazioni che richiedono la configurazione dell'IP pubblico dell'Amministrazione. Si rende opportuno verificare, ogni qualvolta ci si accinge a connettersi al terminal server nella rete del MI, con lo scopo di utilizzare applicazioni come RilP (Rilevazione presenze) e SICOGE, che tale VPN sia attiva.

5.2.9 Gestione e tutela delle password

Si deve proteggere la stazione di lavoro con l'utilizzo di password siano sicure, ovvero complesse, non facilmente individuabili, diverse per l'utenza definita per le attività che afferiscono alla sfera lavorativa da svolgere in smart working. Al momento della modifica delle password evitare di fare solo delle piccole modifiche come numerazioni progressive, ecc.

Esistono sistemi e software open source che consentono un'adeguata sicurezza per la gestione delle password: attraverso un sistema di crittografia molto complesso, questi software sono in grado di salvaguardare le credenziali che vi sono salvate. Un esempio è costituito da "KeePass Password Safe", un software gratuito scaricabile da internet *(v. 8.2.11)*. Si rende noto che è molto più sicuro salvare le proprie password all'interno di un sistema di questo tipo in modo che non siano visibili in chiaro da nessuno al di fuori del proprietario. Questo tipo di software consente altresì la generazione di password sicure e di difficile individuazione.

5.2.10 Hard Disk e dispositivi USB

La possibilità di connettere dispositivi non sicuri al proprio computer utilizzato per il lavoro in smart working, anche solo per copiare o leggere file da una chiavetta USB o da un Hard disk esterno, può comportare l'introduzione di virus sul proprio computer. Per prevenire questo rischio si consiglia di attivare nel proprio antivirus il controllo dei dispositivi esterni e di aggiungere come livello di protezione, la cifratura dei dati inerenti la sfera lavorativa anche su Hard Disk esterni e dispositivi USB.

5.2.11 Tool consigliati

Si riportano di seguito i link diretti per scaricare o utilizzare i prodotti citati nei precedenti paragrafi:

5.2.11.1 Antivirus

Nel caso non si disponga di un antivirus, si consiglia di scaricare Avast antivirus, un software gratuito per ambienti Windows e MAC, che garantisce la protezione del pc e della navigazione in Internet, dal seguente link: https://www.avast.com/it-it/index#pc

5.2.11.2 Blocco Pop-Up

È possibile scaricare e installare il blocco della pubblicità dal seguente link scegliendo la versione relativa al browser di maggiore utilizzo:

https://adblockplus.org/

5.2.11.3 Connessione e accesso a Internet

Per verificare la sicurezza della connessione, gli aggiornamenti relativi al sistema operativo e al browser in utilizzo, è sufficiente cliccare sul seguente link: https://checkme.cyberiskvision.com/check-me

Nel caso dalla scansione emergano anomalie fare click su "Dettagli" e seguire le indicazioni del tool per ovviare agli eventuali problemi legati alla sicurezza della connessione.

5.2.11.4 Gestione e tutela delle password

È possibile installare KeePass Password Safe sia sul computer che su cellulare, in modo da avere sempre a portata di mano tutte le credenziali necessarie. Il link dal quale scaricare l'ultima versione è: https://keepass.info/download.html

5.2.12 Checklist postazioni fisse e notebook

Con lo scopo di verificare di aver apportato tutti gli accorgimenti di sicurezza per ridurre la possibilità di attacchi informatici, viene fornita una checklist che aiuti a tenere traccia delle azioni intraprese e dello stato di sicurezza del computer.

- ☐ Aggiornamento Sistema Operativo
- ☐ Aggiornamento Software
- ☐ Aggiornamento Antivirus
- ☐ Scansione Antivirus
- ☐ Creazione utenza protetta da password
- ☐ Blocco schermo impostato
- ☐ Adblock correttamente installato
- ☐ CheckME effettuato senza anomalie
- ☐ KeePass installato correttamente

5.3 Tablet e Smartphone

5.3.1 Sistema Operativo

Prima di impiegare dispositivi personali in ambito lavorativo è sempre bene verificare che il sistema operativo dello strumento di utilizzo sia aggiornato con le ultime novità in ambito di sicurezza.

Nel caso di un sistema operativo Android, è possibile verificare lo stato degli aggiornamenti di sicurezza tramite i seguenti passaggi: aprire l'app *Impostazioni*, andare su *Sistema*, quindi su *Avanzate* e *Aggiornamento di Sistema;* quindi controllare le sezioni "Versione di Android" e "Livello patch di sicurezza".

Nel caso di un sistema operativo Apple, è possibile verificare lo stato degli aggiornamenti di sicurezza tramite i seguenti passaggi: aprire l'app *Impostazioni,* andare su *Generali*, quindi su *Aggiornamento*

Software.

Qualora il sistema operativo non risultasse aggiornato, è buona norma installare gli aggiornamenti prima di iniziare ad utilizzare il dispositivo.

5.3.2 Applicazioni

Al fine di garantire un buon livello di sicurezza dei device, si ricorda che è opportuno scaricare ed utilizzare solo App ufficiali, presenti nel *Play Store* o nell'*Apple Store*.

È inoltre espressamente vietato immettere credenziali d'accesso e/o dati riservati relativi alla sfera istituzionale in applicazioni non rilasciate ufficialmente dal Fornitore competente, con particolare riguardo alle applicazioni per la gestione della posta elettronica. A tal proposito di seguito viene rilasciato un elenco di applicazioni che l'Amministrazione ritiene idonee per la gestione della posta elettronica delle caselle istituzionali:

- Microsoft Outlook
- Webmail Aruba

Un veloce controllo dello stato di aggiornamento delle applicazioni è utile per aumentare il livello di sicurezza del tablet e dello smartphone.

Nel caso di un sistema operativo Android, è possibile verificare lo stato degli aggiornamenti di sicurezza tramite i seguenti passaggi: aprire l'app *Google Play Store*, andare su *Menu*, quindi su *Impostazioni* e *Aggiornamento automatico app*.

Nel caso di un sistema operativo Apple, è possibile verificare lo stato degli aggiornamenti di sicurezza tramite i seguenti passaggi: aprire l'app *App Store*, nella barra laterale andare su *Aggiornamenti*, quindi su *Aggiorna tutto*.

5.3.3 Blocco Schermo

È sempre buona norma impostare un blocco schermo su tutti i propri apparati. In caso vengano utilizzati smartphone o tablet personali per accedere a dati e caselle istituzionali, è doveroso impostare un blocco schermo tramite PIN o Password (da evitare il blocco schermo sequenza). PIN e Password

devono essere impostate in modo che siano di difficile individuazione tramite azioni di social engineering; sono quindi da evitare nomi, date di nascita o altre informazioni pubbliche. Si consiglia di impostare una sequenza di almeno 8 cifre e non replicare in alcun modo PIN o Password utilizzati su altri servizi.

È altresì consentito utilizzare blocchi biometrici quali il riconoscimento dell'impronta digitale o riconoscimento dell'iride; è invece fortemente sconsigliato il riconoscimento facciale.

Nel caso si disponga di un sistema operativo Android, è possibile impostare il blocco schermo tramite i seguenti passaggi: aprire l'app *Impostazioni*, andare su *Sicurezza*, quindi su *Blocco Schermo*.

Nel caso di un sistema operativo Apple, è possibile impostare il blocco schermo tramite i seguenti passaggi: aprire l'app *Impostazioni*, andare su *Face ID e codice*, quindi su *Attiva Codice*.

5.3.4 Gestione dei documenti

Dispositivi mobili quali smartphone e tablet sono più soggetti a furti o manomissioni rispetto ai computer; pertanto, qualora si decidesse di utilizzare uno di questi device per lavorare da casa, è vietato scaricare i file di lavoro direttamente sul dispositivo. Si rende pertanto opportuno lavorare esclusivamente in Cloud tramite i sistemi forniti dall'Amministrazione.

I dispositivi mobili che supportano la cifratura offrono comunque una maggiore garanzia della protezione di dati eventualmente scaricati o utilizzati in ambito lavorativo. Inoltre, si consiglia di impostare la possibilità di cancellare da remoto il dispositivo in caso di smarrimento o furto.

5.4 Ambienti Cloud

Il Ministero dell'Istruzione fornisce ai dipendenti tutti gli strumenti di lavoro necessari, ivi compresi sistemi cloud per la condivisione di documenti, quali Microsoft OneDrive o SharePoint. I documenti di ambito lavorativo, pertanto, devono essere condivisi unicamente tramite le dotazioni istituzionali.

Non è consentito in nessun caso, l'utilizzo di sistemi cloud non afferenti al MI per la diffusione o la condivisione di documenti lavorativi, anche se inviati ai colleghi con l'autorizzazione per la lettura o modifica dei dati e delle informazioni contenute. Si raccomanda quindi, di condividere tali file

solamente tramite i canali ufficiali di e-mail, chat o condivisione dei documenti esclusivamente al personale che abbia le dovute autorizzazioni.

È pertanto fatto divieto l'utilizzo di sistemi cloud o di posta elettronica personale, per la condivisione e la diffusione delle informazioni e dei documenti afferenti alla sfera lavorativa.

6 Accesso ai servizi

Per accedere ai servizi e alle dotazioni del MI, è sempre necessario un account istituzionale, dotato di nome utente e password. Per evitare la diffusione di dati sensibili volontaria e involontaria, il Ministero dell'Istruzione potrebbe richiedere, in alcuni casi, l'autenticazione a più fattori. Questa pratica aumenta il livello di sicurezza e riservatezza delle informazioni e permette l'accesso solamente al personale del MI, che abbia opportunamente verificato la propria identità; in questo modo, in caso di furto o di smarrimento delle password o delle dotazioni istituzionali ovvero in caso di tentativi di accesso non autorizzati da parte di terzi, le informazioni contenute nei dispositivi e nei servizi offerti dall'Amministrazione godono di un ulteriore strato di protezione.

Per rendere fruibile il servizio di autenticazione a più fattori potrebbe essere richiesto al dipendente di fornire al MI un numero di telefono cui inviare un sms di verifica oppure potrebbe essere richiesta l'installazione di un'apposita applicazione sullo smartphone del personale. In altri casi, invece, l'Amministrazione potrebbe fornire al dipendente un dispositivo che generi un codice OTP di durata temporanea per consentire l'accesso.

Il personale dipendente del Ministero dell'Istruzione ha l'onere di custodire e proteggere al meglio delle proprie possibilità, i sistemi di autenticazione che vengono forniti dall'Amministrazione, ivi comprese credenziali di accesso e le dotazioni su cui vengono configurate le autenticazioni a fattore multiplo. In caso di smarrimento o furto dei dispositivi sopra citati, il personale del MI è tenuto ad informare tempestivamente il proprio Referente Informatico, che provvede a richiedere il blocco o la modifica di tali modalità di accesso.

7 Trattamento dei dati personali

Come noto, sono assegnati al Ministero dell'Istruzione, in forza della missione istituzionale ad esso attribuita, compiti in materia di organizzazione e gestione dell'istruzione scolastica e quanto ad esso connesso, ivi includendo il ruolo di regolazione, supporto e valorizzazione delle autonomie riconosciute alle istituzioni scolastiche (per un quadro sintetico della attività previste nell'ambito del settore dell'istruzione scolastica si rinvia a https://www.miur.gov.it/missione-e-funzione).

Per il corretto ed efficiente adempimento di quanto sopra Il Ministero dell'Istruzione eroga un'ampia gamma di servizi sia in favore del proprio personale che di altri soggetti tra i quali una parte consistente annovera un significativo e diversificato trattamento di dati personali.

Va peraltro rimarcato come, in virtù della platea dei soggetti a cui ciascun servizio o prestazione si riferisca, i dati personali trattati:

- possano far riferimento anche ad un numero estremamente elevato di soggetti (es. docenti, personale ATA ecc.),
- possano far riferimento a soggetti compresi nella fascia di minore età (es. studenti),
- possano comprendere dati di natura particolare laddove riferiti, ad esempio, a fede religiosa, appartenenza sindacale, appartenenza a categorie protette, condizioni di disabilità, patologie in essere o pregresse ecc.

7.1 Trattamento dei dati personali nell'erogazione dei servizi

In generale, ciascun servizio erogato dal Ministero dell'Istruzione o dalle sue strutture organizzative**,** sia per proprio conto, che resi fruibili per conto di terzi,

- è fornito in favore di un'utenza, tra cui il personale stesso in forza al Ministero dell'Istruzione o ad esso temporaneamente trasferito o comandato, le cui caratteristiche, tipologie, esigenze specifiche e perimetri di fruizione sono preliminarmente determinati;
- è erogato con le seguenti particolarità:

- del singolo utente preliminarmente accreditato, tra cui il personale stesso in forza al Ministero dell'Istruzione o ad esso temporaneamente trasferito o comandato, sono acquisiti in via esclusiva o reperiti laddove presenti in archivi già nella disponibilità del MI informazioni che sono salvate su infrastrutture di proprietà del Ministero dell'Istruzione o di fornitori autorizzati del MI allo scopo dell'erogazione dei propri servizi in favore della sola utenza abilitata;
- in relazione all'erogazione dei servizi resi in favore di soggetti minori o altri soggetti deboli o sottoposti a tutela sono acquisite informazioni e concessi accreditamenti attraverso abilitazioni la cui data di scadenza è preliminarmente fissata o sottoposta a periodica verifica della sussistenza delle condizioni per le quali fossero state concesse;
- in relazione agli specifici servizi sono acquisiti e memorizzati dati personali aggiuntivi funzionali all'erogazione da parte del MI delle prestazioni in favore dell'utente o del loro rappresentato;
- a ciascun utente abilitato alla fruizione di servizi erogati dal Ministero dell'Istruzione, tra cui il personale stesso in forza al Ministero dell'Istruzione o ad esso temporaneamente trasferito o comandato, è consentito di aggiornare o di rettificare le informazioni personali ad esso riferite anche allo scopo di modificare o rideterminare il perimetro di fruizione dei servizi. Laddove ciò sia reso possibile anche in virtù di informazioni nella disponibilità del Ministero dell'Istruzione o da esso stesso generate, ciò è effettuato d'ufficio anche in assenza di istanza da parte dello stesso utente;
- al di fuori di quanto direttamente acquisito o archiviato all'interno del proprio perimetro di pertinenza, non è prevista alcuna registrazione da parte del Ministero dell'Istruzione di informazioni o messaggi scambiati tra gli utenti in relazione a servizi o prestazioni erogate o rese fruibili dal Ministero dell'Istruzione

- è supportato da procedure funzionali all'eliminazione di dati relativi ad un utente dei servizi che ne faccia apposita richiesta, purchè non più necessari.

Sia in relazione ai dati personali trattati nel corso dell'erogazione dei propri servizi che per quelli

acquisiti e gestiti per finalità connesse o associate ad altri trattamenti o processi il Ministero dell'Istruzione ha adottato specifiche modalità di gestione. Tali modalità sono consolidate all'interno del **Registro delle attività di Trattamento dati personali** allo scopo di garantire la conformità del Ministero dell'Istruzione stesso e delle sue strutture organizzative alla normativa e, in tal senso, si richiama il rispetto da parte del proprio personale, sia diretto che comandato, sia dei propri collaboratori.

In particolare:

- In relazione ai dati personali di cui il Ministero dell'istruzione sia Titolare al trattamento o Responsabile esterno e di cui il personale, sia diretto che comandato, e i collaboratori del MI potranno venire a contatto (ivi includendo l'eventuale acquisizione effettuata in nome o per conto del MI stesso) sia nel corso dell'esecuzione delle proprie specifiche attività, sia anche in maniera accidentale, ciascuno è esortato ad operare secondo modalità comunque conformi agli artt. 28 - Responsabile del trattamento e 29 - Trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento del GDPR, volendo prevedere, tra gli altri, modalità operative in linea a quelle in uso presso le singole unità organizzative del MI e tali da consentire il rispetto dei Principi riportati al Capo II del citato Regolamento limitatamente a quelli a ciascuno applicabili (*Principi applicabili, Liceità del trattamento, Condizioni per il consenso, Condizioni applicabili ai minori, Trattamento di categorie particolari di dati personali, Trattamento dei dati relativi a condanne penali e reati*);
- in relazione ai dati personali che ciascuno sarà chiamato a trattare nella sua più ampia accezione, ivi includendo i dati personali di natura particolare di qualsivoglia natura, si esorta a:
  - provvederne al trattamento con il massimo scrupolo ed eseguendo le eventuali istruzioni che saranno a voi di volta in volta impartite,
  - assicurare il rispetto dei vincoli di riservatezza, implementando, mantenendo ed all'occorrenza suggerendo l'attuazione di adeguate ed idonee misure tecniche e organizzative,

- garantire il trattamento secondo le modalità indicate nell'apposito Registro dei Trattamenti,
- provvedere a porre all'attenzione dei Responsabili del Ministero dell'Istruzione e delle sue strutture organizzative eventuali suggerimenti di modifiche/integrazioni/rettifiche al Registro dei Trattamenti laddove dovesse rilevarne l'esigenza, anche in virtù dell'attivazione di nuovi trattamenti e/o nuove modalità di trattamento (es. determinate dall'introduzione di nuove soluzioni tecniche/informatizzate),
- nel caso si riscontri una violazione di qualsivoglia natura di dati personali attivare con tempestività iniziative mirate al contenimento o cessazione della violazione rilevata, informare il proprio responsabile circa quanto rilevato e le iniziative fino a quel punto intraprese e, ove necessario, cooperare con il RDP del Ministero dell'Istruzione e, ove necessario, con l'autorità di vigilanza,
- garantirne e far garantire il periodo di conservazione fissato in relazione a ciascuna tipologia di trattamento di dati personali all'interno dell'apposito Registro dei Trattamenti, trascorso il quale, in relazione all'art. 28 comma 3.g), collaborarne alla relativa cancellazione e/o eliminazione, ivi includendo eventuali copie ed elaborazioni effettuate nell'ambito delle attività di specifica pertinenza,
- garantirne modalità di conservazione **sempre all'interno del territorio dell'Unione Europea e preferenzialmente all'interno del territorio italiano**, indipendentemente dalle tipologie di supporti di relativa conservazione/memorizzazione,
- in relazione ai Dati Personali per i quali un soggetto interessato abbia richiesto di esercitarne il diritto alla cancellazione (diritto all'oblio) previsto all'art. 17, supportare la cancellazione "senza ingiustificato ritardo" limitatamente ai soli Dati Personali non soggetti a conservazione in virtù di specifici obblighi di legge e/o la cui eventuale cancellazione potrebbe determinare per il Ministero dell'Istruzione il mancato rispetto di specifici obblighi di legge, una limitazione delle proprie tutele o il difetto di attestabilità di prestazioni o servizi da esso stesso resi,

- partecipare alle sessioni di formazione/informazione sul tema del GDPR e sulle specifiche modalità di trattamento dei dati personali che saranno programmate ed effettuate.

7.2 Conferimento e trattamento dei dati personali da parte del personale del Ministero dell'Istruzione

In relazione al trattamento dei dati personali riferiti al personale in forza o cessato (di seguito personale), il Titolare del trattamento dei dati personali è il Ministero dell'Istruzione, con sede in Roma, in Viale di Trastevere, 76 - 00153, il cui Responsabile della Protezione dei Dati è contattabile all'indirizzo di posta elettronica rpd@istruzione.it .

I dati personali riferiti al personale conferiti al Ministero dell'Istruzione (ivi inclusi quelli a carattere particolare contenuti all'interno del proprio fascicolo ed altra documentazione condivisa con le strutture organizzative del MI) o da esso generati sono e saranno utilizzati nel rispetto dei Principi del Regolamento UE 679/2016 ai fini della gestione del contratto di lavoro e delle prestazioni ad esse connesse e, dunque, laddove il dipendente intendesse opporsi al conferimento/trattamento da parte del MI risulterebbe compromessa la possibilità di dare esecuzione al contratto medesimo ed alla normale esecuzione delle attività in favore dell'Amministrazione.

Il trattamento dei dati personali viene comunque effettuato dal Ministero dell'Istruzione utilizzando procedure e supporti elettronici in conformità ai principi di liceità, correttezza, non eccedenza e pertinenza previsti dalla vigente normativa privacy.

In accordo con l'Art. 5.1 e) del GDPR, il Ministero dell'Istruzione tratterà i dati personali riferiti al proprio personale per tutta la durata di vigenza del rapporto di lavoro in essere e potendoli successivamente mantenere integralmente per ulteriori 10 anni.

In relazione alle finalità del trattamento, l'accesso ai dati personali è consentito a categorie di incaricati dal Ministero dell'Istruzione coinvolti nei trattamenti di relativa pertinenza e potrà comportare anche il conferimento a soggetti terzi (ad esempio i fornitori di servizi IT).

L'elenco aggiornato degli Incaricati e dei Responsabili potrà sempre essere richiesto al Titolare del

Trattamento e/o esaminato all'interno del Registro dei Trattamenti.

Poiché, nel rispetto dei principi statuiti all'interno del Regolamento UE 679/2016, i dati personali relativi al personale costituiscono il presupposto per la gestione del contratto di lavoro, **l'esercizio dei diritti da parte di un dipendente acquisterà la più ampia efficacia al termine del periodo di vigenza** mentre fino a decorrenza di tale data è da intendersi ragionevolmente limitato allo scopo di non arrecare pregiudizio all'Amministrazione.

Ciò premesso, in qualità di soggetto interessato ciascun dipendente avrà la facoltà di esercitare i propri diritti secondo le modalità e nei limiti previsti dalla vigente normativa privacy con diritto di formulare richiesta di:

- accesso: può chiedere conferma dei trattamenti di dati che lo riguardino, nonché di ricevere i dati stessi, nei limiti della ragionevolezza;
- rettifica: il dipendente può chiedere di rettificare o integrare i dati da esso forniti o comunque in possesso dell'Amministrazione, qualora inesatti;
- cancellazione/oblio: il dipendente può chiedere che propri dati acquisiti o trattati dall'Amministrazione siano cancellati, qualora non più necessari alle finalità o laddove non vi siano contestazioni o controversie in essere, in caso di revoca del consenso o opposizione al trattamento, in caso di trattamento illecito, ovvero qualora sussista un obbligo legale di cancellazione;
- limitazione: benché già circoscritta, il dipendente potrà chiedere ulteriore limitazione del trattamento dei suoi dati personali, quando ricorra una delle condizioni di cui all'art. 18 del GDPR; in tal caso, i suoi dati non saranno trattati, salvo che per la conservazione, senza il consenso fatta eccezione per quanto esplicitato nel medesimo articolo al comma 2.
- l'opposizione: il dipendente può opporsi in qualunque momento al trattamento dei suoi dati laddove rilevi l'assenza di motivi legittimi per procederne al trattamento e non ostativi rispetto all'esecuzioni delle sue attività in favore dell'Amministrazione e delle connesse sue attività di coordinamento e di gestione;
- la portabilità: il dipendente può chiedere di ricevere i suoi dati, o di farli trasmettere ad altro titolare da esso indicato, in un formato strutturato, di uso comune e leggibile da dispositivo automatico.

8 Definizioni

Asset: Informazione o risorsa di valore che è necessario salvaguardare.

Attacco alla Sicurezza: Qualsiasi azione volta a compromettere la Sicurezza dell'informazione posseduta da un'organizzazione.

Atti dovuti: circostanze in base alle quali la mancanza di adeguate azioni può comportare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte.

Availability (Disponibilità): Assicurazione che gli utenti autorizzati possano accedere alle informazioni ed alle risorse informatiche quando richiesto.

Browser: programma informatico atto alla navigazione in internet.

Cloud: L'archiviazione, l'elaborazione o la trasmissione dati cui si accede tramite internet protetti da un fornitore esterno.

Confidentiality (Confidenzialità, Riservatezza): Assicurazione che l'informazione è accessibile solo agli utenti autorizzati ad accedervi.

Crack: è un'applicazione che aggira le protezioni di un programma in modo da permetterne l'uso anche non avendolo acquistato.

Data Breach: violazione dei dati personali, rilascio intenzionale o non intenzionale di informazioni sicure o private / riservate in un ambiente non attendibile.

DGSI: Direzione Generale Sistemi Informativi MI.

End-of-life / End-of-support: un termine usato rispetto a un prodotto fornito ai clienti, indicando che il prodotto è alla fine della sua vita utile e che un fornitore interrompe la commercializzazione, la vendita o la rilavorazione per sostenerlo.

Grave e comprovato motivo: evidenza oggettiva, non basata quindi su semplici sospetti o illazioni, che dimostra l'avvenuta violazione di disposizioni di leggi vigenti o delle politiche di sicurezza

dell'Amministrazione.

Information Security (Sicurezza delle Informazioni – SI): Salvaguardia delle caratteristiche di availability, confidentiality e integrity dell'informazione.

Integrity (Integrità): Salvaguardia dell'accuratezza e della completezza dell'informazione e dei beni collegati.

ISMS (Information Security Management System) e SGSI (Sistema di Gestione per la Sicurezza delle Informazioni): Parte del sistema complessivo di gestione, basato su un approccio di business risk, con lo scopo di stabilire, attuare, monitorare, riesaminare, mantenere e migliorare l'information security.

Malware: Programma, documento o messaggio di posta elettronica in grado di apportare danni a un sistema informatico.

Minaccia: Una potenziale causa di danni alle risorse aziendali.

MI: Ministero dell'Istruzione.

Ministero o Amministrazione: si intende il Ministero dell'Istruzione.

Open-source: Software non protetto da copyright e liberamente modificabile dagli utenti.

Password Reuse: La partica di utilizzare password già in uso presso altri account o molto simili tra loro.

Politica: In ISO 9001 e ISO 27001 è la politica, come linea di indirizzo strategico definita dal vertice dell'organizzazione.

Pop-up: Finestre o riquadri, che compaiono automaticamente durante l'uso di un'applicazione ed in determinate situazioni, per attirare l'attenzione dell'utente.

Responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento.

Rischio per la Sicurezza: La possibilità che una certa minaccia sfrutti le vulnerabilità delle risorse aziendali per arrecare danno alle risorse stesse.

Rischio residuo: Il rischio per la Sicurezza che rimane in seguito all'attuazione di tecniche di Sicurezza.

Risk Acceptance (Accettazione del rischio): Decisione di accettare un rischio.

Risk Analysis (Analisi del rischio): Uso sistematico di informazioni per identificare le sorgenti del rischio e per stimare il rischio.

Risk Assessment: Processo complessivo di Risk Analysis e Risk Evaluation: è il processo di identificazione dei rischi per la sicurezza e di individuazione delle loro magnitudo

Risk Evaluation (Valutazione del rischio): Processo di comparazione tra il rischio stimato ed i criteri di rischio stabiliti per determinare la significatività del rischio.

Risk Management (Gestione del rischio): Attività coordinate per dirigere e controllare l'organizzazione in relazione al rischio: è il processo di identificazione e di applicazione di tecniche di Sicurezza all'interno di un'organizzazione (ai sistemi, alle applicazioni ed ai servizi), proporzionali ai rischi Identificati.

Risk Treatment (Trattamento del rischio): Processo per trattare la selezione e l'attuazione delle misure atte a modificare il rischio.

Risorsa aziendale: Tutto ciò che ha un valore per l'azienda: sistemi, applicazioni e servizi

Servizio di Sicurezza: Servizio che garantisce la Sicurezza dei sistemi di elaborazione e di trasmissione dati di un'organizzazione. I servizi di Sicurezza, allo scopo di contenere gli attacchi, utilizzano una o più tecniche di Sicurezza.

Situazioni critiche o di emergenza: circostanze in cui la tempestività d'azione è di fondamentale importanza al fine di evitare danni significativi a cose o persone, perdita di informazioni di rilievo per l'Amministrazione o danni economici e di immagine per l'Amministrazione e per le persone che ne fanno parte o l'interruzione dei servizi informatici e la continuità operativa dei processi dell'Amministrazione.

Software: programma informatico.

Tecnica di Sicurezza: Una procedura, una regola o un meccanismo in grado di ridurre i rischi di Sicurezza.

Trattamento: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

USP: Uffici Scolastici Provinciali.

USR: Uffici Scolastici Regionali (Direzioni Regionali e USP).

Utente: persona fisica abilitata all'utilizzo del servizio di posta elettronica.

VPN: Virtual Private Network (Rete privata virtuale)

Vulnerabilità: Una debolezza in una risorsa o in un gruppo di risorse che può essere sfruttata per arrecare danni alle risorse.

9 Riferimenti normativi

- Regolamento Europeo 27 aprile 2016, n. 679 (GDPR) relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati
- Decreto Legislativo n. 101/2018 – Adeguamento al Regolamento UE 2016/679
- Decreto Legislativo n. 82/2005 – Codice dell'amministrazione digitale
- Decreto Legislativo n. 196/2003 e s.m.i. – Codice in materia di protezione dei dati personali.
- Provvedimento del Garante per la protezione dei dati personali n. 157 del 30 luglio
- Legge 124/2015 in materia di riorganizzazione delle amministrazioni pubbliche.
- Legge 248/2000 in materia di tutela del diritto d'autore.