POLITICHE

PER LA SICUREZZA

DELLE INFORMAZIONI

PER GLI UTENTI DEL SISTEMA INFORMATIVO DELL'ISTRUZIONE

PER I DOCENTI

1. RIFERIMENTI GENERALI

1.1 Traccia delle versioni

numero versione	**data ultima modifica**
v. 2.0	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 docente del Ministero dell'Istruzione che utilizzi il servizio di posta elettronica del dominio *@posta.istruzione.it.*

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.

Nel cap. 3 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.

Il cap. 4 informa gli utenti sulle modalità di accesso ai servizi dell'amministrazione.

Il cap. 5 informa gli utenti sul trattamento dei dati personali, esteso a tutte le casistiche di cui sopra.

I cap. 6 e 7 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. 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.

3.1 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.

3.2 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.

3.3 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.

3.4 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.

3.4.1 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.

3.4.2 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.

4. 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.

5. 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.

5.1 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:

o 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;

o 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;

o 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;

o 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;

o 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.

5.2 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.

6. 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.

7. 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.