Allegato 6

Piano di sicurezza del sistema di gestione informatica dei documenti

Premessa

Il presente piano di sicurezza, che è parte integrante del manuale di gestione, è adottato ai sensi delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici nel rispetto delle misure minime di sicurezza stabilite da AgID nella circolare 2/2017, nel rispetto delle disposizioni in materia di protezione dei dati personali e nel rispetto delle disposizioni in materia di continuità operativa dei sistemi operativi.

Il piano di sicurezza descrive le politiche adottate dall'**Istituto Comprensivo "Palmanova - Destra Torre"**

affinché

- i documenti e le informazioni trattati dalla scuola siano resi accessibili, integri e riservati;
- i dati personali comuni, sensibili e giudiziari vengano custoditi in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Il piano di sicurezza, in base ai rischi cui sono esposti i dati (personali e non) e i documenti trattati, definisce:

- le minime di sicurezza adottate dall'Istituto Comprensivo "Palmanova - Destra Torre" attraverso il documento Analisi misure minime di sicurezza informatica presente nel portale GDPR app
- le modalità di accesso al Sistema di Gestione Informatica dei Documenti (SGID) Madisoft;
- le modalità di accesso alle funzionalità del SGID;
- le modalità di accesso ai dati e ai documenti contenuti nel SGID;
- le modalità di tracciamento di ogni evento di modifica;
- gli interventi operativi adottati sotto il profilo organizzativo, procedurale e tecnico, al fine di garantire le misure di sicurezza necessarie alla tutela del patrimonio documentale dell'Ente e alla tutela e garanzia dei dati personali, sensibili e giudiziari;

- la formazione degli addetti;
- le modalità con le quali deve essere effettuato il monitoraggio periodico delle misure di sicurezza e il loro miglioramento.

Il piano di sicurezza è soggetto a revisione a seguito di particolari esigenze, determinate da sopravvenienze normative o evoluzioni tecnologiche.

Elementi di rischio cui sono soggetti i documenti informatici e i dati contenuti nel Sistema di Gestione Informatica dei Documenti

I principali elementi di rischio cui sono soggetti i documenti informatici e i dati trattati con l'ausilio delle tecnologie informatiche sono essenzialmente riconducibili alle seguenti tipologie:

- accesso non autorizzato al SGID, alle funzioni del SGID e ai dati e documenti in esso contenuti;
- cancellazione, manomissione o perdita dei dati e documenti presenti nel SGID;
- trattamento illecito, eccedente rispetto allo scopo o comunque non in linea con la normativa vigente, dei dati personali.

Per prevenire tali rischi e le conseguenze da essi derivanti, l'Istituto Comprensivo Rovigo 2 adotta gli accorgimenti e le politiche per la sicurezza di seguito descritte.

Sicurezza del sistema in cloud

Il SGID è installato in cloud, accessibile dalla rete intranet dell'Ente, ereditando dalla stessa tutti i meccanismi da questa previsti per la protezione dei dati. L'infrastruttura tecnologica è certificata ISO / IEC 9001, ISO /IEC 27001.

Procedure comportamentali degli operatori ai fini della protezione dei documenti informatici e dei dati in essi contenuti

Le postazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, di proprietà dell'Istituto a vario titolo messi a disposizione del personale, sono strumenti di lavoro e il loro utilizzo è finalizzato allo svolgimento delle attività professionali e istituzionali dell'Ente.

Ogni operatore adotta comportamenti corretti, tali da preservare il buon funzionamento degli strumenti e da ridurre i rischi per la sicurezza dei sistemi informativi.

Gli operatori cui sono affidati i dispositivi informatici di proprietà dell'Istituto sono tenuti ad avere le seguenti accortezze:

- qualora nei dispositivi e nelle postazioni di lavoro siano memorizzati dati sensibili e giudiziari, l'operatore che li utilizza deve porre in atto comportamenti idonei a garantire la protezione di detti dati;
- ciascun operatore è tenuto a segnalare immediatamente ai referenti informatici ogni sospetto utilizzo non autorizzato, violazione della sicurezza o malfunzionamento relativo ai dispositivi informatici a lui assegnati;
- al momento della cessazione del rapporto di lavoro, ciascun operatore deve restituire all'Istituto qualsiasi risorsa informatica a lui assegnata e mettere a disposizione ogni informazione di interesse istituzionale;
- non è consentito installare programmi non inerenti all'attività lavorativa;
- non è consentito copiare dati la cui titolarità sia dell'Istituto su dispositivi esterni personali se non autorizzati dal Dirigente scolastico.

Ai fini della vigilanza nell'utilizzo degli strumenti informatici assegnati, ciascun operatore ha l'obbligo di impedire ad altri l'utilizzo non autorizzato della propria apparecchiatura informatica.
Le stazioni di lavoro, da tavolo e portatili, o gli strumenti comunque funzionalmente assimilabili, messi a disposizione del personale, non devono essere lasciati incustoditi. L'operatore è tenuto a bloccare o a spegnere il personal computer in caso di sospensione o termine dell'attività lavorativa e, comunque sempre, al termine dell'orario di servizio.

Accesso al SGID da parte dei dipendenti

L'accesso al SGID da parte dell'unità organizzativa della segreteria avviene attraverso l'utilizzo di credenziali di autenticazione.
Le credenziali di autenticazione consistono in un codice (*User-Id*), per l'identificazione dell'incaricato, associato ad una parola chiave riservata (*Password*), conosciuta solamente dal medesimo. Tali credenziali vengono verificate in tempo reale da un apposito sistema di identificazione, il quale consente l'accesso ai soggetti abilitati e traccia tutti gli accessi di ciascun utente, memorizzando, ai fini di controllo, l'*User-Id* corrispondente, ma non la *Password* dello stesso.
Agli incaricati è prescritto di adottare le necessarie cautele volte ad assicurare la segretezza della *Password*. La password, assegnata in automatico la prima volta, deve essere cambiata dall'utente al primo accesso e poi quando richiesto dal sistema.
Se la password viene digitata in modo errato per cinque volte, l'utente viene disabilitato.

Lo stesso *User-Id* non può essere assegnato ad altri incaricati neppure in tempi diversi. Le credenziali non utilizzate non si disattivano automaticamente ma devono essere disabilitate manualmente.

La password degli utenti scade ogni sei mesi quindi, in caso di inutilizzo, questa scade e ne deve essere impostata una nuova per poter riattivare l'utenza.

Qualora il titolare delle credenziali di autenticazione dimenticasse la propria *password* si procederà all'assegnazione di una nuova chiave di accesso utilizzando la funzione "reimposta password".

Le credenziali di accesso sono strettamente personali e ogni attività non regolare effettuata e riconducibile alle stesse è imputata al titolare delle credenziali medesime.

Accesso alle funzionalità del SGID da parte di utenti

I profili di abilitazione alle funzionalità del SGID sono attribuiti a ciascun utente dal responsabile della gestione documentale, o suo vicario, nel rispetto del principio dei minimi privilegi in base al quale devono essere assegnati a ciascun utente solo i privilegi necessari per svolgere le attività di competenza.

I privilegi di amministratore devono essere limitati ai soli utenti che abbiano competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.

Protezione dei documenti contenenti dati personali, sensibili e giudiziari

Sui documenti protocollati contenenti dati personali, sensibili e giudiziari può essere inserito un livello di riservatezza. Il protocollo riservato rende il documento e i suoi metadati visualizzabili solo agli utenti compresi nell'ACL (lista controllo accessi) generata con l'assegnazione. Gli altri utenti non compresi nell'ACL vedono i metadati cifrati e non hanno possibilità di accedere al documento. Il livello di riservatezza può essere impostato anche sul fascicolo al momento della sua apertura. In questo caso gli utenti non presenti nella ACL non solo non visualizzano i documenti contenuti nel fascicolo, ma nemmeno la sua "camicia" virtuale, vale a dire i metadati identificativi del fascicolo (oggetto, responsabile, numero, data di apertura ecc.). Il SGID consente inoltre la gestione degli omissis negli atti anche ai fini della pubblicazione in Amministrazione Trasparente.

In caso di violazione dei dati personali si deve contattare il DPO e nei casi più gravi alla notifica al garante entro 72 ore e alla comunicazione all'interessato nel rispetto degli art. 33 e 34 del GDPR.

Tracciamento di ogni evento di modifica e di ogni attività svolta

Il Sistema consente l'effettuazione di qualsiasi operazione sui dati, documenti, fascicoli in esso contenuti, esclusivamente agli utenti abilitati per lo svolgimento di ciascuna attività; il Sistema effettua, inoltre, il tracciamento di qualsiasi evento di modifica delle informazioni trattate e di tutte le attività rilevanti ai fini della sicurezza svolte su di esso da ciascun utente, in modo da garantirne l'identificazione; tali registrazioni (log di sistema) sono protette al fine di non consentire modifiche non autorizzate. I dati registrati nei file di log sono raccolti, memorizzati e conservati dal sistema informatico in conformità alla normativa vigente. Le informazioni contenute nei file di log possono essere messe a disposizione dell'autorità giudiziaria, la quale può richiedere la non cancellazione e la conservazione di tali file per un periodo più lungo di quanto disposto dalla legge.

Difese contro i malware

Il Sistema e tutti i documenti e dati in esso contenuti sono protetti contro i rischi di intrusione non autorizzata e contro l'azione di programmi informatici mediante l'attivazione di software antivirus e firewall, regolarmente aggiornati con aggiornamento automatico. Ai fini di ridurre la vulnerabilità dei sistemi informativi, il sistema operativo utilizzato dal dipendente e il SGID vengono costantemente tenuti aggiornati, per mezzo dell'istallazione degli aggiornamenti periodici che i fornitori rendono disponibili.

Backup

Il Backup dei dati contenuti nel SGID avviene in cloud direttamente dalla software house.
Il Backup dei dati e documenti presenti sui server locali avviene ogni giorno con un backup incrementale sulla Nas in locale.

Trasmissione e interscambio dei documenti

La trasmissione e l'interscambio di documenti e fascicoli informatici all'interno dell'Istituto avviene per mezzo del SGID, della rete lan locale; nessun'altra modalità è consentita, al fine di evitare la dispersione e la circolazione incontrollata di documenti e dati. La mail è usata solo per le comunicazioni informali tra dipendenti.
La trasmissione di documenti informatici al di fuori dell'Ente avviene tramite PEC o PEO a seconda del destinatario e del livello di tracciabilità che si vuole ottenere.
Nel caso di comunicazioni tramite e-mail contenenti allegati con informazioni sensibili, i documenti verranno crittografati.

Le informazioni relative alla segnatura di protocollo sono strutturate in un file XML conforme alle specifiche contenute nell'allegato 6 delle Linee Guida AgID relative alla produzione, gestione e conservazione del documento informatico.

Conservazione dei documenti

I documenti informatici registrati sul SGID sono affidati per la conservazione digitale ad un soggetto conservatore qualificato dall'AgID, che svolge tale attività in conformità a quanto sancito dalle regole contenute nelle Linee guida AgID. Il trasferimento in conservazione avviene mediante la produzione di pacchetti di versamento, basati su uno schema XML conforme a quanto previsto nello stesso manuale di conservazione.

Disaster recovery

Il disaster recovery (DR) è un elemento fondamentale nella strategia di gestione della continuità operativa, specialmente per le organizzazioni che lavorano con dati sensibili o critici. Si riferisce a un insieme di politiche, strumenti e procedure progettati per garantire il ripristino dei sistemi IT e dei dati aziendali a seguito di un evento catastrofico.
Per quanto concerne il Sistema di Gestione Informatica dei Documenti (SGID) il link del fornitore (Madisoft) è: https://supporto.madisoft.it/portal/it/kb/articles/come-scaricare-i-documenti-privacy-e-policy-di-sicurezza-termini-e-condizioni

Il backup dei dati è il seguente:

- **Backup Locale**, che consiste nel salvare copie dei dati su supporti fisici come dischi rigidi esterni, NAS (Network Attached Storage) o server locali. Questa soluzione è veloce e accessibile, ma presenta il rischio di perdita dei dati in caso di disastri fisici come incendi o alluvioni.

Accesso di Utenti esterni al Sistema

L'esercizio del diritto di accesso da parte di utenti esterni al Sistema viene effettuato nel rispetto di quanto sancito dalla legge 241/90 e s.m.i., dal D.Lgs. 33/2013 e s.m.i., dal D. Lgs. 196/03 e s.m.i. e del Regolamento Europeo sulla Protezione dei Dati n. 679 del 2016 (GDPR).

Piani formativi del personale

Ai fini di una corretta gestione documentale e di garantire la sicurezza informatica, l'Ente predispone apposite attività formative per il personale.

Monitoraggio periodico delle misure di sicurezza in materia di gestione documentale

Il Responsabile della gestione documentale dell'ente effettua periodiche verifiche sul corretto funzionamento del SGID, valutando a tal fine, anche per mezzo di controlli a campione, il corretto svolgimento delle operazioni inerenti la gestione documentale. I Log di sistema sono comunque conservati e protetti in modo da consentire successive verifiche che dovessero risultare necessarie sullo svolgimento di tutte le operazioni rilevanti al fine della sicurezza dei dati, effettuate sul sistema.

Misure di tutela e garanzia

In conformità all'art. 28 del GDPR, **Modisoft,** fornitrice del SGID, è individuata come responsabile del trattamento dei dati.