Ministero dell'Istruzione e del Merito

ISTITUZIONE SCOLASTICA IC MACCARESE

Piano della sicurezza del sistema di gestione informatica dei documenti

1. Oggetto e Finalità

Il presente piano definisce - in attuazione delle Linee Guida Agid (Agenzia per l'Italia Digitale", *"Linee guida sulla formazione, gestione e conservazione dei documenti informatici*" (maggio 2021) secondo cui le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017 - le misure tecniche e organizzative adottate per garantire un livello di sicurezza adeguato al rischio, con particolare riferimento alla riservatezza, integrità e disponibilità dei dati trattati nel sistema di gestione documentale.

2. Figure coinvolte nella predisposizione del Piano

In conformità al modello organizzativo scolastico, le figure coinvolte sono:

- **Dirigente Scolastico (DS):** rappresenta legalmente l'Istituto e approva il presente Piano, assumendo la responsabilità finale del trattamento dei dati (Titolare), e le strategie di mitigazione dei rischi informatici;
- **Direttore dei Servizi Generali e Amministrativi (DSGA):** Sovraintende all'applicazione delle misure organizzative da parte del personale ATA e collabora all'assegnazione dei profili di autorizzazione.
- **Amministratore di Sistema (AdS):** Cura l'attuazione tecnica delle misure di sicurezza (configurazione firewall, backup, aggiornamenti hardware/software) e monitora i log di sistema.

- **Responsabile della gestione documentale**: predispone il piano in accordo con gli altri responsabili.
- **Responsabile della conservazione**: collabora per garantire che le misure di sicurezza siano mantenute durante l'intero ciclo di vita del documento.
- **Responsabile per la transizione digitale (RTD)**: coordina l'integrazione tecnologica delle misure.
- **Responsabile della protezione dei dati (RPD)**: fornisce parere obbligatorio sulle misure adottate e sorveglia l'osservanza del GDPR.

3. Informazioni trattate nel sistema di gestione documentale e sistemi utilizzati

1. **Dati Amministrativi e Contabili:** gestiti tramite i software di segreteria Madisoft Nuvola e il sistema documentale.
2. **Dati Didattici e di Valutazione:** gestiti attraverso l'applicazione del Registro Elettronico.
3. **Piattaforme di Collaborazione e Didattica a Distanza:** Account istituzionali di docenti e studenti (es. *Google Workspace / Microsoft 365*).
4. **Infrastruttura Locale:** Rete LAN/Wi-Fi dell'istituto, postazioni PC degli uffici di segreteria, dei laboratori didattici e dei dispositivi di plesso.

4. Analisi dei Rischi

L'Istituzione scolastica valuta i rischi derivanti da:

- Distruzione o perdita (anche accidentale) dei documenti.
- Accesso non autorizzato o trattamento non conforme alle finalità.
- Modifica o divulgazione non autorizzata di dati personali, con particolare attenzione alle categorie particolari di dati ex artt. 9-10 del GDPR (dati ex sensibili e giudiziari),

5. Misure di Sicurezza Tecniche previste (ex art. 32 GDPR)

In osservanza del disposto di cui all'art. 32 del Regolamento (UE) 2016/679, l'Istituzione scolastica per la gestione dei flussi documentali e mitigare i rischi connessi al trattamento dei dati personali adotta le seguenti misure di sicurezza Tecniche:

- **Pseudonimizzazione e Cifratura**: tecniche applicate ai dati personali per ridurre l'identificabilità dell'interessato in caso di violazione. In particolare, la cifratura dei dati in transito e a riposo è garantita dai fornitori delle piattaforme SaaS in uso (Registro Elettronico, Protocollo) certificati e qualificati sul Cloud Marketplace di AgID/ACN.
- **Autenticazione** a due fattori per l'accesso ai sistemi critici della scuola (registro elettronico, cloud di segreteria, console di gestione delle email istituzionali come Google Workspace o Microsoft 365 ecc.).
- **Backup** periodici dei dati, su base giornaliera, salvati su supporti diversi, con una copia off site/cloud disconnessa dalla rete ordinaria per proteggersi dai ransomware.
- **Resilienza dei Sistemi**: Capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

- **Protezione degli endpoint e della rete** mediante installazione di antivirus/antimalware su tutti i PC della segreteria e Dirigenza; segmentazione della rete Wi-Fi (la rete per la didattica/studenti deve essere totalmente separata da quella della segreteria).
- **Disaster Recovery**: Procedure per il ripristino tempestivo dell'accesso ai dati in caso di incidente fisico o tecnico.
- **Certificati SSL/HTTPS**: Adozione di certificati di sicurezza per i siti web istituzionali che gestiscono flussi di dati
- Procedure per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- Verifica periodica della conformità delle attrezzature informatiche ai requisiti di sicurezza previsti dalla normativa vigente e dai protocolli interni adottati.

6. Misure di Sicurezza Organizzative (ex art. 32 GDPR)

In osservanza del disposto di cui all'art. 32 del Regolamento (UE) 2016/679, l'Istituzione scolastica per la gestione dei flussi documentali e mitigare i rischi connessi al trattamento dei dati personali adotta altresì le seguenti misure di sicurezza Organizzative:

- **Controllo degli Accessi (Profili di Autorizzazione)**:
    - L'accesso ai documenti è limitato ai soggetti autorizzati in base alle competenze amministrative o didattiche.
    - obbligo di modificare la password al primo accesso, divieto di condivisione delle credenziali e di trascrizione delle stesse su supporti cartacei visibili;
    - Per la **protocollazione riservata**, la visibilità completa è limitata all'assegnatario e agli operatori con permessi specifici.
    - Blocco automatico delle sessioni di lavoro dopo 5 (cinque) minuti di inattività su tutte le postazioni di segreteria e Dirigenza.
- **Istruzioni Operative**: Notifica a tutto il personale autorizzato al trattamento dei dati, delle istruzioni operative sul corretto trattamento dei dati personali effettuato con o senza l'ausilio di attrezzature informatiche;
- **Formazione**: formazione periodica per il personale autorizzato circa i rischi e le procedure di sicurezza.
- **Audit e Test**: Procedure per verificare e valutare regolarmente l'efficacia delle misure tecniche.
- Redazione e notifica a tutto il personale autorizzato al trattamento dei dati, di regolamenti interni, manuali, istruzioni operative utili alla gestione corretta dei documenti, per la tutela dei dati personali in essi contenuti.
- Redazione delle valutazioni di impatto per tutti quei trattamenti che lo richiedono.

7. Gestione delle Categorie Particolari di Dati

Per i documenti contenenti dati ex art. 9 del Regolamento UE 679/2016 (es. certificati medici, dati su disabilità degli alunni, provvedimenti giudiziari):

- l'operatore incaricato è tenuto a contrassegnare il documento come "contenente dati riservati" all'atto della protocollazione;

- il sistema deve garantire l'oscuramento dei dati del profilo (come la classificazione) agli utenti privi di diritti di accesso specifici;
- i dati particolari dovranno essere conservati limitatamente al tempo strettamente necessario previsto dal piano di conservazione e scarto.
- i fascicoli degli alunni con disabilità (PEI) o DSA (PDP) gestiti in modalità informatica, è limitato tramite partizionamento delle cartelle cloud esclusivamente al rispettivo Consiglio di Classe/Team docenti e alle figure di supporto (Funzioni Strumentali), inibendo la visualizzazione al restante personale docente dell'istituto, previa anonimizzazione della documentazione documentazione stessa.

8. Procedura per violazione dei dati personali (data breach)

Ai sensi degli artt. 33 e 34 del GDPR, in caso di violazione di dati personali (es. accesso abusivo, perdita di dati, attacco ransomware), le fasi di cui consta la procedura sono le seguenti:

1. **Rilevazione:** segnalazione immediata al Dirigente Scolastico e al DPO (Data Protection Officer).
2. **Valutazione:** analisi della gravità e del numero di interessati coinvolti.
3. **Notifica all'Autorità Garante:** se la violazione presenta un rischio per i diritti e le libertà, la notifica deve avvenire tempestivamente, **entro e non oltre le 72 ore** dalla conoscenza.
4. **Comunicazione agli Interessati:** obbligatoria se il rischio è considerato "elevato" (es. furto di dati sanitari degli alunni).
5. **Registro delle Violazioni:** ogni incidente, anche se non notificato al Garante, deve essere verbalizzato e annotato in un registro interno con l'indicazione delle misure correttive adottate. Il Registro delle Violazioni è custodito in formato digitale protetto dal Dirigente Scolastico e aggiornato tempestivamente con il supporto del RPD.

9. Monitoraggio e Aggiornamento

Il presente Piano è parte integrante del Manuale di gestione documentale. Viene aggiornato con cadenza almeno annuale per garantire la coerenza con l'evoluzione tecnologica e con i nuovi indirizzi del Piano Triennale per l'Informatica nella PA.

Il presente Piano, a seguito dell'adozione formale da parte del Dirigente Scolastico, viene portato a conoscenza degli Organi Collegiali (Collegio dei Docenti e Consiglio d'Istituto) per gli aspetti di rispettiva competenza, e viene diffuso a tutto il personale della scuola tramite i canali di comunicazione istituzionali.

Letto e acquisito il parere del Responsabile della Protezione dei Dati (DPO)

Il Responsabile della gestione documentale

_____

Il Responsabile della Conservazione documentale

_____