Allegato 6 – Piano della sicurezza del Sistema di Gestione Documentale.

APPROVAZIONE DEL PIANO

Il presente Piano della Sicurezza del Sistema di Gestione Documentale (SGD) è stato redatto ai sensi del Codice dell'Amministrazione Digitale, delle Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici e della normativa vigente in materia di protezione dei dati personali.

Il documento costituisce parte integrante del Sistema di Gestione Documentale dell'Istituto ed entra in vigore dalla data della sua approvazione.

1. Introduzione e Quadro Normativo

Il presente Piano della Sicurezza del Sistema di Gestione Documentale (SGD) definisce le misure organizzative, procedurali e tecniche adottate dall'Istituto per garantire la riservatezza, l'integrità, la disponibilità, l'autenticità e la tracciabilità dei documenti informatici e dei dati trattati attraverso il Sistema di Gestione Documentale Argo Gecodoc, erogato in modalità SaaS (Software as a Service) da Argo Software S.r.l.

Il Piano disciplina le modalità di gestione della sicurezza del sistema documentale, individuando ruoli, responsabilità, misure di prevenzione, procedure di controllo e intervento in caso di incidenti di sicurezza, nel rispetto della normativa vigente in materia di amministrazione digitale, protezione dei dati personali e sicurezza informatica.

Lo scopo del documento è integrare le misure di sicurezza infrastrutturali e tecnologiche garantite dal Responsabile del Trattamento (Argo Software S.r.l.) con le misure organizzative e procedurali poste in essere dal Titolare del Trattamento, assicurando un adeguato livello di protezione del patrimonio documentale dell'Istituto e la continuità dei processi amministrativi.

Il presente Piano costituisce parte integrante del Sistema di Gestione Documentale dell'Istituto ed è coordinato con il Manuale di Gestione Documentale, il Manuale di Conservazione, il Registro dei Trattamenti previsto dal Regolamento (UE) 2016/679 e le ulteriori disposizioni organizzative interne in materia di sicurezza delle informazioni.

La predisposizione e l'aggiornamento del Piano sono curati dal Responsabile della Gestione Documentale, d'intesa con il Responsabile della Conservazione e previo coinvolgimento del Responsabile della Protezione dei Dati (RPD/DPO). Il documento è sottoposto a revisione periodica almeno annuale o in occasione di modifiche normative, organizzative o tecnologiche rilevanti.

1.1 Riferimenti Normativi Principali

Il presente Piano è redatto nel rispetto della seguente normativa e documentazione di riferimento:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio (GDPR);
- Decreto Legislativo 7 marzo 2005, n. 82 e successive modificazioni (Codice dell'Amministrazione Digitale - CAD);

- Decreto Legislativo 30 giugno 2003, n. 196 e successive modificazioni (Codice in materia di protezione dei dati personali);
- Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici;
- Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente;
- Misure e indirizzi di cybersicurezza emanati dall'Agenzia per la Cybersicurezza Nazionale (ACN);
- Manuale di Gestione Documentale dell'Istituto;
- Manuale di Conservazione adottato dall'Ente;
- Security Policy e documentazione tecnica del fornitore Argo Software S.r.l.

1.2 Obiettivi DEL Piano

Il Piano della Sicurezza del Sistema di Gestione Documentale persegue i seguenti obiettivi:

- garantire la riservatezza, l'integrità, la disponibilità, l'autenticità e la tracciabilità dei documenti informatici e dei dati trattati attraverso il Sistema di Gestione Documentale;
- assicurare la corretta gestione dei documenti durante l'intero ciclo di vita, dalla formazione alla conservazione;
- definire in modo chiaro ruoli, responsabilità, procedure operative e misure di sicurezza applicabili al sistema documentale;
- garantire la conformità alla normativa vigente in materia di amministrazione digitale, protezione dei dati personali e sicurezza delle informazioni;
- prevenire accessi non autorizzati, perdita, alterazione o divulgazione indebita dei dati e dei documenti;
- promuovere l'adozione di adeguate misure organizzative e tecniche per la gestione dei rischi informatici e documentali;
- assicurare la continuità operativa dei processi amministrativi e documentali;
- definire procedure per la rilevazione, la gestione e la risoluzione degli incidenti di sicurezza;
- favorire la consapevolezza del personale attraverso attività di formazione e aggiornamento in materia di sicurezza informatica e gestione documentale.

2. Ambito di Applicazione

Il presente Piano si applica:

- al Sistema di Gestione Documentale adottato dall'Istituto e alle relative componenti applicative;
- a tutti gli utenti autorizzati all'accesso e all'utilizzo del sistema;
- all'infrastruttura tecnologica utilizzata per l'erogazione del servizio, inclusi gli ambienti cloud e i servizi correlati;
- ai processi di formazione, registrazione, protocollazione, classificazione, fascicolazione, archiviazione, conservazione e accesso ai documenti informatici;
- ai documenti amministrativi informatici, ai fascicoli elettronici e alle aggregazioni documentali;

- ai dati personali, compresi quelli appartenenti a categorie particolari ai sensi del Regolamento (UE) 2016/679;
- alle attività svolte dal personale interno, dai soggetti autorizzati e dai fornitori coinvolti nella gestione del sistema documentale.

Le disposizioni contenute nel presente Piano si applicano a tutti i trattamenti di dati e documenti effettuati nell'ambito delle attività istituzionali dell'Istituto mediante il Sistema di Gestione Documentale.

3. Struttura Organizzativa e Responsabilità

La sicurezza del Sistema di Gestione Documentale (SGD) è garantita attraverso la chiara attribuzione di ruoli, compiti e responsabilità ai soggetti coinvolti nella gestione documentale, nella protezione dei dati personali e nella sicurezza delle informazioni.

Ruolo	Responsabilità Principali
Titolare del Trattamento (Istituto Scolastico)	Definisce le finalità e le modalità del trattamento dei dati personali, adotta le misure organizzative necessarie per garantire la sicurezza del sistema, autorizza gli utenti all'accesso, vigila sul rispetto delle procedure interne e assicura la conformità normativa dell'Ente.
Responsabile del Trattamento (Argo Software S.r.l)	Garantisce la sicurezza dell'infrastruttura tecnologica e dei servizi erogati in modalità SaaS, assicura l'adozione delle misure tecniche di protezione dei dati, la continuità operativa, le procedure di backup e disaster recovery, nonché il rispetto degli obblighi previsti dal contratto e dalla normativa vigente.
Responsabile della Gestione Documentale	Sovrintende al corretto funzionamento del sistema documentale, cura l'aggiornamento del Manuale di Gestione Documentale e del presente Piano, coordina le attività di protocollazione, classificazione, fascicolazione e gestione dei flussi documentali.
Responsabile della Conservazione	Garantisce il corretto svolgimento del processo di conservazione dei documenti informatici, verificando la conformità alle disposizioni normative e alle procedure adottate dall'Ente.
Responsabile della Protezione dei Dati (RPD/DPO)	Supporta l'Istituto scolastico nella verifica della conformità al Regolamento (UE) 2016/679, fornisce consulenza in materia di protezione dei dati personali, monitora l'applicazione delle misure di

	sicurezza e partecipa alla gestione degli eventuali incidenti di sicurezza e data breach.
Amministratori del servizio	Gestiscono le utenze, i profili di autorizzazione, la configurazione e la parametrizzazione del sistema; effettuano controlli periodici sugli accessi e operano nel rispetto del principio del minimo privilegio. Gli amministratori sono formalmente individuati e autorizzati dall'Ente.
Utenti Autorizzati	Utilizzano il sistema nell'ambito delle proprie competenze istituzionali, gestiscono documenti, fascicoli e cartelle, applicano correttamente le procedure di protocollazione, classificazione, fascicolazione e riservatezza, e sono tenuti al rispetto delle disposizioni contenute nel presente Piano.

Tutti i soggetti coinvolti nella gestione del Sistema di Gestione Documentale operano secondo il principio di responsabilizzazione (accountability), adottando comportamenti conformi alle disposizioni normative, alle procedure interne e alle misure di sicurezza previste dall'Ente.

Le responsabilità attribuite ai singoli ruoli sono formalizzate mediante specifici atti di nomina, incarico o autorizzazione, conservati agli atti dell'Istituto.

4. Misure Tecniche e Infrastrutturali

Le misure tecniche e infrastrutturali descritte nel presente capitolo sono garantite da Argo Software S.r.l., in qualità di Responsabile del Trattamento e fornitore del Sistema di Gestione Documentale erogato in modalità SaaS (Software as a Service).

Tali misure sono finalizzate a garantire la riservatezza, l'integrità, la disponibilità e la resilienza dei dati e dei documenti gestiti dall'Istituto, in conformità alla normativa vigente e alle politiche di sicurezza adottate dal fornitore.

4.1 Architettura e Protezione dei Dati

- Hosting e localizzazione dei dati

I database, i repository documentali e le copie di backup del Sistema di Gestione Documentale sono ospitati presso infrastrutture cloud AWS (Amazon Web Services), ubicate all'interno dello Spazio Economico Europeo, nelle regioni Europa (Irlanda) ed Europa (Milano), nel rispetto della normativa europea in materia di protezione dei dati personali.

- Crittografia dei dati

I dati archiviati nei database, nei repository documentali e nelle copie di backup sono protetti mediante algoritmi di cifratura avanzata basati sullo standard AES-256 (Advanced Encryption Standard), al fine di garantirne la riservatezza e la protezione da accessi non autorizzati.

- Protezione dei dati in transito

Le comunicazioni tra utenti e sistema avvengono mediante protocolli sicuri HTTPS/TLS, che assicurano la cifratura dei dati durante la trasmissione sulle reti telematiche.

4.2 Continuità Operativa e Disaster Recovery

- Ridondanza e resilienza

L'infrastruttura tecnologica garantisce adeguati livelli di ridondanza e resilienza attraverso la replica dei sistemi e dei dati su differenti zone di disponibilità (Availability Zone) della piattaforma cloud, riducendo il rischio di indisponibilità del servizio.

- Backup e conservazione delle copie di sicurezza

Sono effettuati backup automatici giornalieri comprendenti snapshot dei dati e registrazione delle transazioni.

Le copie di sicurezza sono conservate secondo le seguenti modalità:

  - backup giornalieri conservati per 35 giorni;
  - backup settimanali conservati per ulteriori 25 giorni.

- Versionamento dei documenti

È attiva la funzionalità di versionamento dei documenti che consente il recupero e il ripristino delle versioni precedenti dei file archiviati, contribuendo alla tutela dell'integrità documentale e alla gestione degli errori operativi.

- Parametri di Disaster Recovery

In caso di eventi che compromettano la disponibilità del servizio, il fornitore garantisce i seguenti livelli di servizio:

- RTO (Recovery Time Objective): tempo massimo di ripristino del servizio pari a 4 ore;
- RPO (Recovery Point Objective): perdita massima teorica di dati limitata a 24 ore rispetto all'ultimo backup disponibile.

4.3 Misure Tecnologiche di Sicurezza

Al fine di garantire un adeguato livello di protezione del sistema sono adottate le seguenti misure:

- registrazione e conservazione dei log relativi agli accessi e alle operazioni effettuate dagli utenti;
- monitoraggio dei sistemi e delle infrastrutture;
- aggiornamento periodico dei componenti software;
- applicazione delle patch di sicurezza rilasciate dai produttori;
- manutenzione preventiva e correttiva dell'infrastruttura tecnologica;
- adozione di misure di protezione contro accessi non autorizzati e vulnerabilità note.

4.4 Gestione dell'Autenticazione e delle Autorizzazioni

- Controllo degli accessi basato sui ruoli (RBAC)

L'accesso alle funzionalità del sistema è regolato mediante un modello di controllo degli accessi basato sui ruoli (Role Based Access Control – RBAC), che consente di attribuire a ciascun utente esclusivamente le autorizzazioni necessarie allo svolgimento delle proprie mansioni.

- Principio del minimo privilegio

Le autorizzazioni assegnate agli utenti sono limitate ai soli privilegi strettamente necessari per l'esercizio delle attività istituzionali, secondo il principio del minimo privilegio.

- Protocolli di autenticazione

Le procedure di autenticazione utilizzano protocolli standard sicuri basati su OAuth 2.0.

- Autenticazione forte

Il sistema consente l'utilizzo di modalità di autenticazione forte, tra cui SPID di livello 2 e ArgoID.

L'Istituto promuove l'adozione di credenziali ad elevato livello di sicurezza e delle modalità di autenticazione maggiormente affidabili messe a disposizione dal fornitore.

- Gestione delle password

Le credenziali di accesso sono protette mediante algoritmi di hashing conformi alle raccomandazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN) e alle buone pratiche internazionali in materia di sicurezza informatica.

5. Misure Organizzative e di Gestione (Responsabilità dell'Ente)

Le misure organizzative descritte nel presente capitolo disciplinano le modalità di utilizzo del Sistema di Gestione Documentale da parte del personale autorizzato e definiscono le procedure adottate dall'Istituto per garantire la sicurezza applicativa, la corretta gestione delle autorizzazioni e la protezione dei dati trattati.

5.1 Gestione degli Accessi

- Identificazione degli utenti

L'accesso al Sistema di Gestione Documentale è consentito esclusivamente mediante credenziali personali e nominative.

È espressamente vietato l'utilizzo di account condivisi, generici o intestati a più soggetti.

Ogni utente è responsabile della custodia delle proprie credenziali e del corretto utilizzo delle funzionalità alle quali è autorizzato.

- Utilizzo del Single Sign-On (SSO)

L'utilizzo delle funzionalità di autenticazione persistente ("Ricordami") è consentito esclusivamente su dispositivi personali e adeguatamente protetti.

In caso di utilizzo di postazioni condivise o accessibili ad altri utenti, il personale è tenuto a effettuare il logout al termine di ogni sessione di lavoro.

- Gestione delle autorizzazioni

Le autorizzazioni di accesso sono assegnate e gestite dagli utenti incaricati della gestione delle utenze attraverso gli strumenti messi a disposizione dal fornitore.

L'attribuzione dei profili di accesso avviene nel rispetto del principio del minimo privilegio e in relazione alle effettive esigenze operative dell'utente.

Il sistema prevede i seguenti profili di autorizzazione:

- Amministratore (Abilitato a tutte le funzioni)

Consente l'accesso completo alle funzionalità del sistema, comprese:

- gestione documentale;
- gestione fascicolare;
- documenti riservati;

- modifiche autorizzate;
- invio in conservazione;
- configurazione e parametrizzazione del sistema.

Tale profilo deve essere attribuito esclusivamente a personale espressamente autorizzato dal Dirigente Scolastico.

- Abilitato alla gestione documentale

Consente la gestione dei documenti informatici secondo le autorizzazioni assegnate.

- Abilitato alla gestione documentale e fascicolare

Consente la gestione dei documenti e delle aggregazioni documentali, comprese cartelle e fascicoli.

- Abilitato alla conservazione

Consente l'accesso alle funzionalità di conservazione e alle operazioni di invio dei documenti al sistema di conservazione.

- Abilitato alle modifiche autorizzate

Consente l'esecuzione delle modifiche previste dalla normativa e dalle procedure interne sui documenti protocollati.

L'attribuzione di tale profilo avviene sotto la responsabilità dell'Istituto e deve essere limitata ai casi strettamente necessari.

- Accesso ai documenti riservati

Consente la consultazione e la gestione dei documenti classificati come riservati.

- Abilitato alla trasmissione e importazione dei fascicoli

Consente la trasmissione e la ricezione di fascicoli informatici tra amministrazioni abilitate.

- Abilitato alla parametrizzazione

Consente la configurazione delle funzionalità del sistema e la gestione dei repertori documentali.

- Associazione utenti-uffici

Gli utenti devono essere associati agli uffici di competenza in modo da limitare l'accesso esclusivamente ai documenti, fascicoli e cartelle pertinenti alle attività svolte.

L'associazione è effettuata dagli amministratori del sistema secondo l'organizzazione interna dell'Istituto.

- Revisione periodica delle autorizzazioni

Le autorizzazioni assegnate agli utenti sono sottoposte a verifica periodica almeno una volta all'anno e ogniqualvolta intervengano modifiche organizzative, trasferimenti di personale o cessazioni del servizio.

- 5.2 Classificazione dei Dati

I documenti e le informazioni gestiti attraverso il Sistema di Gestione Documentale possono contenere:

- dati identificativi;
- dati amministrativi;
- dati personali;
- categorie particolari di dati ai sensi dell'articolo 9 del Regolamento (UE) 2016/679.

I documenti contenenti dati particolari o informazioni soggette a particolari esigenze di tutela sono classificati come riservati.

L'accesso a tali documenti è consentito esclusivamente al personale specificamente autorizzato mediante appositi profili di accesso.

- 5.3 Gestione della Riservatezza dei Documenti
- Corrispondenza riservata

In caso di acquisizione o importazione nel Sistema di Gestione Documentale di documenti o messaggi contenenti dati personali particolari, dati giudiziari o altre informazioni soggette a particolari vincoli di riservatezza, l'operatore deve classificare correttamente il documento come "riservato" utilizzando le funzionalità previste dal sistema.

- Configurazione delle tipologie documentali

Le tipologie documentali, i fascicoli, i modelli e le altre aggregazioni documentali sono configurati dagli amministratori del sistema tenendo conto:

- del livello di riservatezza;
- degli uffici competenti;

- della classificazione archivistica;
- delle esigenze di accessibilità e consultazione.
- Principio di riservatezza

Tutti gli utenti autorizzati sono tenuti a trattare dati e documenti nel rispetto dei principi di riservatezza, minimizzazione e protezione dei dati personali previsti dalla normativa vigente.

È vietata qualsiasi consultazione, estrazione o diffusione di documenti non strettamente connessa alle attività istituzionali svolte.

6. Misure Organizzative, Formazione e Gestione degli Incidenti

L'Istituto adotta specifiche misure organizzative finalizzate a garantire il corretto utilizzo del Sistema di Gestione Documentale, la protezione delle informazioni trattate e il mantenimento di adeguati livelli di sicurezza nel tempo.

6.1 Gestione degli Utenti e dei Privilegi

L'Istituto definisce procedure formalizzate per la gestione dell'intero ciclo di vita delle utenze, dalla loro attivazione fino alla cessazione o modifica delle autorizzazioni.

In particolare sono previste:

- l'attivazione delle utenze esclusivamente a seguito di autorizzazione del Dirigente Scolastico o del soggetto delegato;
- la tempestiva modifica o revoca delle autorizzazioni in caso di trasferimento, cambio mansione o cessazione del rapporto di servizio;
- la verifica periodica delle utenze attive e dei relativi privilegi di accesso;
- la documentazione delle operazioni di attivazione, modifica e disattivazione delle utenze;
- il rispetto del principio del minimo privilegio nell'assegnazione delle autorizzazioni.

Le autorizzazioni assegnate agli utenti sono sottoposte a revisione periodica almeno annuale e ogniqualvolta intervengano modifiche organizzative rilevanti.

Tutto il personale autorizzato all'utilizzo del Sistema di Gestione Documentale è tenuto a partecipare alle attività formative previste dall'Istituto in materia di sicurezza informatica, protezione dei dati personali e gestione documentale.

6.2 Consapevolezza e Formazione

L'Istituto promuove la diffusione della cultura della sicurezza informatica e della corretta gestione documentale attraverso attività periodiche di informazione, formazione e aggiornamento del personale.

Le attività formative riguardano in particolare:

- la protezione dei dati personali e gli obblighi derivanti dal Regolamento (UE) 2016/679;
- il corretto utilizzo del Sistema di Gestione Documentale;
- la gestione delle credenziali di accesso;
- i rischi derivanti da phishing, malware, ransomware e altre minacce informatiche;
- le procedure interne di classificazione, protocollazione, fascicolazione e conservazione dei documenti;
- le misure di sicurezza previste dal presente Piano.

La partecipazione alle attività formative è registrata e documentata dall'Istituto.

6.3 Gestione degli Incidenti di Sicurezza

Per incidente di sicurezza si intende qualsiasi evento che possa compromettere la riservatezza, l'integrità, la disponibilità o l'autenticità dei dati, dei documenti o dei servizi informatici dell'Istituto.

- Segnalazione degli incidenti

Qualsiasi anomalia, sospetto accesso non autorizzato, perdita di dati, malfunzionamento rilevante o violazione della sicurezza deve essere segnalata tempestivamente al Dirigente Scolastico, al DSGA e al Responsabile della Protezione dei Dati (RPD/DPO).

- Registro degli incidenti

Tutti gli incidenti di sicurezza sono registrati in apposito Registro degli Incidenti, nel quale vengono annotati:

- data e ora dell'evento;
- soggetti coinvolti;
- descrizione dell'incidente;
- impatti rilevati;
- misure adottate;

- esito delle attività di gestione e ripristino.

- Processo di gestione degli incidenti

La gestione degli incidenti segue il seguente processo:

Rilevazione → Segnalazione → Classificazione → Contenimento → Mi□gazione → Ripris□no → Verifica finale → Chiusura dell'evento

Per ogni incidente vengono individuate le azioni necessarie per limitare gli effetti dell'evento e ripristinare nel più breve tempo possibile la normale operatività.

- Gestione delle violazioni dei dati personali (Data Breach)

Qualora l'incidente comporti una violazione dei dati personali, il Titolare del Trattamento procede alla valutazione dell'evento con il supporto del RPD/DPO.

Nei casi previsti dalla normativa vigente, la violazione viene notificata al Garante per la Protezione dei Dati Personali entro 72 ore dalla sua conoscenza e, ove necessario, agli interessati coinvolti.

- Analisi e miglioramento continuo

Al termine della gestione dell'incidente viene effettuata un'analisi finalizzata a:

- individuare le cause dell'evento;

- valutare l'efficacia delle misure adottate;

- definire eventuali azioni correttive e preventive;

- aggiornare procedure, configurazioni o misure di sicurezza ove necessario.

Le risultanze dell'analisi sono conservate agli atti dell'Istituto e utilizzate per il miglioramento continuo del sistema di gestione della sicurezza documentale.

7. Matrice di Valutazione dei Rischi

La valutazione dei rischi è effettuata considerando l'impatto potenziale sull'attività dell'Istituto e la probabilità di accadimento dell'evento. Il livello di rischio è determinato sulla base della combinazione di tali fattori e consente di individuare le misure di mitigazione da adottare.

ID	Area di rischio	Evento rischioso	Impatto (1-5)	Probabilità (1-5)	Livello rischio	Misure di mitigazione
R1	Accessi non	Consultazione di dati	4	2	3	Profilazione rigorosa

	autorizzati	personali, documenti riservati o fascicoli da parte di soggetti non autorizzati.			(Medio)	degli utenti, attribuzione dei ruoli secondo il principio del minimo privilegio, autenticazione forte (SPID/CIE ove disponibile), verifica periodica delle autorizzazioni.
R2	Integrità dei dati	Alterazione, danneggiamento o cancellazione accidentale di documenti e registrazioni informatiche.	5	1	2 (Basso)	Backup automatici, versionamento dei documenti, controlli sugli accessi, verifica periodica della possibilità di ripristino dei dati.
R3	Continuità operativa	Interruzione del servizio causata da guasti hardware, blackout elettrici, problemi di rete o indisponibilità temporanea dei servizi cloud.	3	3	4 (Medio)	Utilizzo di infrastrutture ridondate, procedure di disaster recovery, gruppi di continuità (UPS) per le postazioni critiche e monitoraggio dei servizi.
R4	Errore umano	Errata protocollazione, classificazione, fascicolazione o conservazione dei documenti.	3	2	2 (Basso)	Formazione periodica del personale, procedure operative documentate, controlli a campione e affiancamento del personale neoassegnato.
R5	Conservazione a lungo termine	Obsolescenza dei formati documentali o perdita della validità	5	1	2 (Basso)	Utilizzo di formati standard e aperti (PDF/A), conservazione

		giuridica dei documenti conservati.				digitale a norma e monitoraggio periodico dei processi di conservazione.
R6	Attacco ransomware	Cifratura o blocco dei documenti e dei dati a seguito di attacco informatico.	5	3	4 (Alto)	Backup periodici, aggiornamento dei sistemi, formazione anti-phishing, autenticazione forte e monitoraggio degli accessi.
R7	Violazione dei dati personali (Data Breach)	Accesso, divulgazione o perdita non autorizzata di dati personali trattati dall'Istituto.	5	2	4 (Alto)	Controllo degli accessi, cifratura dei dati, registrazione dei log, procedure di gestione degli incidenti e notifica al Garante nei casi previsti dalla normativa.
R8	Indisponibilità del fornitore cloud	Temporanea indisponibilità dei servizi erogati dal fornitore SaaS o problemi infrastrutturali esterni.	4	2	3 (Medio)	Garanzie contrattuali di continuità operativa, sistemi di backup, procedure di disaster recovery e monitoraggio dei livelli di servizio (SLA).

7.1 Riesame della Valutazione dei Rischi

La valutazione dei rischi è sottoposta a riesame periodico almeno con cadenza annuale, al fine di verificare l'efficacia delle misure di sicurezza adottate e l'adeguatezza del livello di protezione garantito dal Sistema di Gestione Documentale.

Il riesame è altresì effettuato ogni qualvolta si verifichino una o più delle seguenti condizioni:

- modifiche significative dell'organizzazione interna dell'Istituto;
- introduzione di nuovi sistemi informatici, servizi digitali o funzionalità del Sistema di Gestione Documentale;
- aggiornamenti normativi o regolamentari che incidano sui processi documentali o sul trattamento dei dati personali;

- verificarsi di incidenti di sicurezza, violazioni dei dati personali (data breach) o altri eventi rilevanti sotto il profilo della sicurezza delle informazioni;
- aggiornamento delle infrastrutture tecnologiche o delle modalità di erogazione del servizio;
- variazioni dei processi amministrativi e documentali che comportino nuovi rischi o modifiche ai rischi esistenti.

L'esito del riesame è formalizzato in apposito verbale o relazione interna e costituisce elemento di aggiornamento del presente Piano della Sicurezza, nonché delle ulteriori procedure e misure organizzative adottate dall'Istituto.

8. Monitoraggio, Revisione e Aggiornamento del Piano

8.1 Monitoraggio

L'Istituto assicura il monitoraggio periodico dell'efficacia delle misure organizzative, procedurali e tecniche previste dal presente Piano, al fine di garantire il mantenimento di adeguati livelli di sicurezza del Sistema di Gestione Documentale.

Le attività di monitoraggio comprendono:

- verifica periodica delle autorizzazioni e dei privilegi di accesso assegnati agli utenti;
- controllo dell'applicazione delle procedure organizzative e di sicurezza;
- verifica della corretta gestione dei documenti riservati;
- monitoraggio degli incidenti di sicurezza e delle azioni correttive adottate;
- verifica dell'efficacia delle attività di formazione e sensibilizzazione del personale;
- controllo dell'aggiornamento della documentazione correlata al Sistema di Gestione Documentale.

8.2 Revisione e Aggiornamento del Piano

Il presente Piano della Sicurezza è sottoposto a revisione almeno una volta all'anno da parte del Responsabile della Gestione Documentale, in collaborazione con il Responsabile della Conservazione e con il Responsabile della Protezione dei Dati (RPD/DPO).

L'aggiornamento del Piano è obbligatorio nei seguenti casi:

- modifiche significative dell'infrastruttura tecnologica o dei servizi digitali utilizzati dall'Istituto;
- introduzione di nuove funzionalità o modifiche sostanziali del Sistema di Gestione Documentale;
- aggiornamento della valutazione dei rischi;
- rilevazione di vulnerabilità significative o incidenti di sicurezza rilevanti;
- modifiche normative o regolamentari che incidano sulla gestione documentale o sulla protezione dei dati personali;
- variazioni organizzative che comportino modifiche ai ruoli, alle responsabilità o ai processi documentali.

Ogni aggiornamento del Piano è registrato nel Registro delle Revisioni e approvato secondo le procedure interne dell'Istituto.

- 8.3 Conservazione della Documentazione

Il presente Piano, unitamente alle successive revisioni, è conservato agli atti dell'Istituto in formato digitale e reso disponibile ai soggetti autorizzati che ne abbiano necessità per ragioni di servizio.

9. Allegati

Costituiscono parte integrante del presente Piano i seguenti documenti:

- Procedura di Backup e ripristino dati;
- Registro delle emergenze del Protocollo Informatico
- Valutazione dei Rischi relativa al Sistema di Gestione Documentale (art.7)
- Policy di sicurezza del fornitore Argo Software S.r.l.;
- Registro dei Trattamenti dei dati personali;

Gli allegati sono aggiornati secondo le rispettive procedure di gestione e conservati unitamente alla documentazione del Sistema di Gestione Documentale.

La Dirigente Scolastica
Enrica Romano
Documento firmato digitalmente