LICEO ARTISTICO STATALE - "BRUNO MUNARI"
VIA GANDHI 14 - 31029 VITTORIO VENETO (TV)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Elaborato in base al D.LGS. 30 giugno 2003 n.196 in "MATERIA DI PROTEZIONE DEI DATI PERSONALI"
ed al relativo disciplinare tecnico

INDICE

ALLEGATI AL DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

A. NATURA E LUOGHI DI RESIDENZA DEI DATI, FINALITÀ E MODALITÀ DEL TRATTAMENTO AUTORIZZATE, TIPOLOGIE DI COMUNICAZIONE E DIFFUSIONE AMMESSE

1. Personale amministrativo
   Banca Dati: ALUNNI
   Banca Dati: PERSONALE
   Banca Dati: CONTABILITA'
   Banca Dati: FORNITORI DI BENI E SERVIZI
   Banca Dati: PROTOCOLLO
2. Personale docente
3. Collaboratori scolastici

B. LINEE GUIDA IN MATERIA DI SICUREZZA DEI DATI

1. Istruzioni operative per la sicurezza dei dati – Personale Docente, amministrativo e tecnico, collaboratore scolastico
2. Disciplinare interno per l'utilizzo delle strumentazioni informatiche, della rete Internet e della posta elettronica da parte del personale e degli studenti

C. INCARICATI DEL TRATTAMENTO E MANUTENTORI DEL SISTEMA

D. TUTELA DEI DIRITTI DELL'INTERESSATO

1. Informativa
2. Procedura di accesso

Il Dirigente dell'Istituzione Scolastica

Visto il decreto legislativo 30 giugno 2003, n. 196 recante il Codice in materia di protezione di dati personali, e segnatamente gli art. 34 ss., nonché l'allegato B del suddetto D.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

Considerato che l'Istituzione Scolastica: Liceo Artistico Statale "Bruno Munari" con sede in via Gandhi n.14, a Vittorio Veneto, Provincia di Treviso, in quanto dotata di un autonomo potere decisionale, ai sensi dell'art. 28 del d.lgs. n. 196 del 2004, deve ritenersi titolare del trattamento di dati personali;

Atteso che la suddetta Istituzione scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli art. 31 e ss. Del d.lgs. n. 196 del 2003;

Adotta il presente Documento programmatico sulla sicurezza dei dati redatto ai sensi e per gli effetti dell'articolo 34, comma 1, lettera g) del D.Lgs. 196/2003 e del disciplinare tecnico allegato B

1. Scopo del documento e applicabilità

Scopo di questo Documento Programmatico per la Sicurezza nel seguito indicato come DPS, è di delineare i criteri, le modalità operative e le misure organizzative, fisiche e logiche adottate dall'Istituto per garantire:

a. la disponibilità delle informazioni per gli utenti del sistema, compatibilmente con i livelli di servizio;
b. l'integrità delle informazioni, che quindi possono essere create, modificate o cancellate solo dalle persone autorizzate a svolgere tali operazioni;
c. l'autenticità e la garanzia della provenienza dei dati;
d. la riservatezza delle informazioni, che possono essere fruite solo dalle persone autorizzate.

In questo documento vengono definiti in particolare:

- l'elenco dei trattamenti di dati personali;
- i tipi di dati trattati;
- la descrizione delle aree, dei locali e degli strumenti con i quali si effettuano i trattamenti;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- i modi per individuare e valutare i rischi;
- l'analisi dei rischi che incombono sui dati;
- le misure adottate per garantire l'integrità e la disponibilità dei dati e la sicurezza delle trasmissioni;
- nonché la protezione delle aree e dei locali;
- i criteri e le modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- gli interventi formativi previsti per gli incaricati del trattamento;
- i criteri da adottare in caso di affidamento del trattamento a soggetti esterni all'Istituto;
- le modalità di verifica e valutazione delle misure adottate.

Le indicazioni contenute nel presente documento devono essere utilizzate per gestire i rischi connessi alle attività di trattamento dei dati personali, sia in seno all'Istituto che da parte dei responsabili esterni.

2. Caratteristiche dell'Istituto

4.1. Le persone

Gli alunni iscritti ai corsi sono n. 464

L'organico del personale:

- docente, compreso il personale che presta servizio anche in altre istituzioni scolastiche, è costituito da n. 73 Docenti;
- A.T.A. consta di n. 20 unità così distribuite:
  - n. 1 Direttore dei servizi generali ed amministrativi,
  - n. 6 assistenti amministrativi,
  - n. 4 assistenti tecnici,
  - n. 9 collaboratori scolastici.

4.2. Le strutture

La scuola è così articolata:

SEDE N. 1 - centrale sita nel comune di Vittorio Veneto in Via Gandhi n.14.

Struttura dell'edificio:

Il sito è circondato da una protezione perimetrale con cancelli d'accesso che sono sorvegliati durante le ore di attività e chiusi a fine giornata lavorativa. Inoltre l'edificio è circondato non su tutti i lati da fari illuminanti nel periodo notturno. Dispone inoltre di fari anche per l'illuminazione di lati o cortili interni.

La sede principale non è difesa nelle porte d'accesso e nelle finestrature con vetri antisfondamento o inferriate.

L'edificio di recente costruzione si presenta efficiente sia per quanto concerne gli impianti tecnologici che relativamente alla struttura architettonica interna.

I locali dove vengono trattati dati personali, sia per mezzo di documenti cartacei che attraverso applicazioni ed archivi informatici, sono situati all'interno dell'area dedicata agli uffici il cui accesso è sempre presidiato durante il normale svolgimento dell'attività lavorativa.

Misure di sicurezza (TU81/2008)

Il sistema antincendio è costituito da estintori manuali a polvere ed anidride carbonica omologati. E' garantita la manutenzione con controllo d'efficienza semestrale da parte di una società specializzata e si provvede ad assicurare la continuità nell'addestramento di personale preposto sull'uso degli estintori stessi.

Inoltre la sede è provvista di rilevatori di fumo ubicati nei seguenti locali:

piano terra: aula polifunzionale, aule 11, 12, 13, 14, 15, laboratorio 16, e relativo corridoio

piano primo: aula magna, biblioteca, sala insegnanti, ufficio di presidenza, vicepresidenza, dsga, segreteria didattica e segreteria contabile, corridoio ala uffici

piano secondo: aule 42, 43, laboratori 40, 41 e relativo corridoio

E' stato predisposto un piano d'evacuazione, sono ubicati nei punti necessari e visibili al pubblico le procedure scritte in caso d'emergenza, è funzionante l'impianto d'illuminazione d'emergenza nei locali d'accesso al pubblico.

Alimentazione elettrica e sistemi di continuità

L'impianto elettrico è a norma come anche la cablatura della rete informatica. Esiste la dichiarazione di conformità firmata dall'installatore. È presente l' impianto di messa a terra che è sottoposto a regolare manutenzione.

E' presente per le postazioni di lavoro e il server un sistema d'alimentazione, specifico, dedicato, separato dagli altri contesti utilizzatori e con potenza adeguata, che soddisfa la necessaria continuità elettrica di funzionamento.

3. Responsabilità

I responsabili, gli incaricati del trattamento e i manutentori del sistema sono individuati con apposito provvedimento che specifica finalità e modalità del trattamento autorizzate nonché tipologie di comunicazione e diffusione ammesse (**Allegato C**).

4.3. Titolare del trattamento

Titolare del trattamento è il Liceo Artistico Statale "Bruno Munari", con sede in via Gandhi n. 14, a Vittorio Veneto Provincia di Treviso, nella veste del suo rappresentante legale pro-tempore, il Dirigente Scolastico Prof.ssa Franca Braido.

Il Dirigente Scolastico in qualità di titolare del trattamento dei dati

- è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione di misure di sicurezza, sia idonee che minime;
- procede alla predisposizione delle misure idonee ritenute indispensabili nella struttura, valuta la congruità tecnico-economica delle misure proposte e quindi disporre l'adozione delle stesse;

- individua il/i responsabile/i del trattamento e con apposito incarico ne stabilisce le responsabilità in merito al rispetto degli adempimenti e delle prescrizioni stabiliti sulla base del D.Lgs.vo 196/03;
- si avvale della collaborazione del D.S.G.A. e dei responsabili dei diversi settori per la predisposizione della modulistica e delle procedure.

4.4. Responsabile del trattamento

Al responsabile del trattamento sono attribuiti incarichi di ordine organizzativo e direttivo, ed egli provvede a:

- individuare e designare per iscritto gli incaricati del trattamento che operano sotto la sua diretta autorità indicando puntualmente l'ambito del trattamento consentito;
- impartire loro specifiche istruzioni scritte relative alle modalità di trattamento ammesse;
- organizzare la formazione per gli incaricati;
- procedere alle verifiche specificate nell'incarico.

E' individuato quale Responsabile del trattamento dei dati comuni e sensibili:

Sig.ra Lucia Magnano per	Docenti
	Organi Collegiali
	Collaboratori del Preside
	Personale ATA

4.5. Amministratore di Sistema

Il Titolare del trattamento conferisce l'incarico di Amministratore di Sistema al soggetto incaricato di sovrintendere alle Risorse Informatiche dell'Istituto secondo quanto stabilito nel **Disciplinare interno (Allegato B)** per l'utilizzo delle strumentazioni informatiche, della rete internet e della posta elettronica.

L'Amministratore di Sistema, nell'espletamento delle sue funzioni legate alla sicurezza e alla manutenzione informatica, ha facoltà di accedere in qualunque momento, anche da remoto, e dopo aver richiesto l'autorizzazione all'utente interessato, al personal computer di ciascun dipendente.

4.6. Incaricati del trattamento

L'assegnazione del personale docente e ATA alla specifica unità operativa, per la quale è individuato con atto formale, comporta l'automatico incarico al trattamento autorizzato per iscritto agli addetti all'unità medesima e la consegna, a cura del Responsabile del Trattamento, delle specifiche istruzioni scritte relative alle modalità di trattamento ammesse.

Per il personale amministrativo la designazione per iscritto riguarda un singolo incaricato e con essa si individua l'ambito del trattamento a questi consentito.

Di norma tali incarichi sono assegnati a partire dal 1° settembre, data di inizio del nuovo anno scolastico che coincide con le assegnazioni di sede del personale. Al presente documento è allegato l'elenco dei provvedimenti adottati con i relativi estremi (**Allegato C**).

Sia per i trattamenti effettuati con strumenti elettronici, che per quelli che avvengono senza l'ausilio di tali strumenti, l'autorizzazione al trattamento è soggetta ad aggiornamento periodico e comunque almeno annuale, quando viene verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione riguardo l'ambito di trattamento consentito sia ai singoli incaricati che agli addetti alla manutenzione e gestione degli strumenti elettronici.

4. Dati e banche dati

Al fine di elaborare l'elenco dei trattamenti dei dati, posti in essere dal Titolare:

- sono precisate le finalità del trattamento;
- sono individuati i tipi di dati personali trattati, in base alla loro natura (comuni, giudiziari o sensibili ed alla categoria di soggetti cui essi si riferiscono (alunni, personale dipendente, fornitori)
- sono definite le operazioni di trattamento dei dati effettuate;
- sono descritte le aree, i locali e gli strumenti con i quali si effettuano i trattamenti.

4.7. Finalità del trattamento

Al fine di perseguire le finalità istituzionali, il Liceo Artistico Statale "Bruno Munari" effettua operazioni di trattamento di dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori con le seguenti finalità:

a. la selezione e il reclutamento del personale a tempo determinato, nonché l'instaurazione, la gestione e la cessazione del rapporto di lavoro;
b. la frequenza dei corsi di studio;
c. l'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami;
d. l'attivazione degli organismi collegiali e delle commissioni istituzionali previsti dall'ordinamento scolastico;
e. l'acquisizione di beni, servizi e opere;
f. la difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrative, nonché quelle connesse alla gestione degli affari penali e civili;
g. le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche.

4.8. Tipologie di dati trattati

Il Liceo Artistico Statale "Bruno Munari", con salvezza della possibilità di procedere a successive integrazioni e/o correzioni, tratta **i dati personali di natura comune o sensibile** di seguito elencati:

a. Dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del d.lgs. n.196 del 2003, univocamente riconducibili ad un soggetto fisico, identificato o identificabile, quali nominativo, dati di nascita, residenza, domicilio, stato di famiglia, codice fiscale, stato relativo all'adempimento degli obblighi di leva.
b. Dati identificativi, ai sensi dell'art.4, comma 1, lettere b) e c) del d.lgs. n.196 del 2003, univocamente riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la sede, la Partita IVA, il Codice fiscale, la titolarità di diritti o la disponibilità di beni strumentali;
c. Dati sensibili e giudiziari di cui all'art.4, comma 1, lett.d) del d.lgs. n.196 del 2003 così come descritti nelle schede allegate al D.M. 305 del 7.12.'06 e relativi a origine, convinzioni religiose, filosofiche, politiche e sindacali, stato di salute e vita sessuale.
d. Dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi individualizzati differenziati;
e. Dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;
f. Dati atti a rilevare la presenza presso l'istituzione scolastica dei destinatari dell'offerta formativa ovvero dei famigliari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale offerta;
g. Dati inerenti negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni;
h. Dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;
i. Dati contabili e fiscali;
j. Dati inerenti la titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;
k. Dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

I dati trattati da questa amministrazione sono noti all'istituzione scolastica, in ragione della produzione di atti e/o dichiarazioni raccolti per iniziativa degli interessati a fruire direttamente, o a beneficio dei minori sottoposti alla potestà ex art. 316 c.c., dei servizi formativi o previa richiesta dell'Ufficio presso medesimi ovvero presso altri soggetti pubblici e privati in particolare attraverso:

- documenti contabili connessi alla fornitura di prestazioni e/o di servizi e/o di lavori;
- documentazione bancaria, finanziaria e/o assicurativa;
- documenti inerenti il rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/o previdenziali;
- pubblici registri, elenchi, atti o documenti conoscibili da chiunque.

I dati sono accolti e conservati su supporti cartacei e/o informatici e organizzati nelle seguenti banche dati:

- banca dati alunni;
- banca dati personale direttivo, insegnante e ATA a tempo indeterminato e determinato;
- banca dati fornitori (beni e servizi);
- banca dati – contabilità;
- banca dati - protocollo

per ognuna delle quali è predisposta una scheda di processo allegata al presente documento (**Allegato A**). I documenti e le banche dati settoriali allocate nelle varie postazioni di lavoro ricadono per le operazioni di salvataggio, condivisione e comunicazione significativa sotto la responsabilità dei diversi incaricati. Il sistema di abilitazioni dispone l'utilizzo delle informazioni ai soli utilizzatori cui ricade la competenza.

4.9. Operazioni di trattamento dei dati effettuate

Sono considerate operazioni di trattamento dei dati quelle di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione dei dati stessi oltre ad interconnessione e raffronti con altro titolare anche effettuate mediante strumenti elettronici.

Delle operazione di trattamento sono incaricati gli operatori individuati annualmente con apposita nomina che contestualmente precisa le operazioni autorizzate in relazione alle banche dati e alle modalità di trattamento (informatizzato e non).

4.10. Aree, locali e archivi ove risiedono i dati e strumenti con i quali si effettuano i trattamenti

Il trattamento dei dati è effettuato nei seguenti locali:

- Ufficio di Presidenza
- Ufficio di Vice Presidenza/Funzioni Strumentali
- Ufficio del DSGA
- Ufficio di segreteria didattica, magazzino, protocollo
- Ufficio di segreteria contabile, personale

Archiviazione cartacea

I documenti sono conservati:

1. Archivio storico;
2. Ufficio del Dirigente scolastico (armadi, schedari, computer);
3. Ufficio del DSGA (armadi, schedari, armadio blindato, computer)
4. Ufficio della Didattica, Magazzino, Protocollo, nell'archivio corrente (schedari, armadi, computer);
5. Ufficio della Contabilità, Personale nell'archivio corrente (schedari, armadi, computer).

Gli uffici sono chiudibili a chiave.

Gli armadi per la custodia e l'archiviazione di atti, documenti e supporti, con particolare riferimento a quelli contenenti dati sensibili o giudiziari sono adeguati a garantire la necessaria sicurezza ai dati personali contenuti negli atti, documenti e supporti ivi conservati in quanto muniti di apposite serrature e chiavi

È presente una cassaforte destinata anche al ricovero dei supporti contenenti le copie di sicurezza delle banche dati informatiche. Essa è ubicata nell'ufficio del DSGA, locale diverso da quello del server.

Strumentazioni informatiche

La situazione attuale delle attrezzature informatiche è la seguente:

Locale	Numero postazioni	anno acquisto	Trattamenti effettuati
Ufficio di presidenza	1	2010	F-secure client security
Ufficio di vicepresidenza/funzioni	1	2005	F-secure client security

strumentali	1	2006	F-secure client security
Ufficio del dsga	1	2008	F-secure client security
Ufficio didattica, magazzino, protocollo	2	2004	F-secure client security
	1	2007	F-secure client security
	1	2008	F-secure client security
Ufficio contabilità, personale	1	2010	F-secure client security
	1	2005	F-secure client security
Totale	**10**		

Il sistema è costituito da cablaggio strutturato e certificato. Il cablaggio rispetta la certificazione in cat. 5e.

Il sistema informativo è basato su server che ospita le banche dati in modo da attuare il maggior grado di tutela e salvaguardia delle stesse.

Il server è ubicato nell'ufficio segreteria didattica. Il locale è normalmente presidiato dal personale amministrativo e soggetto a regolare chiusura.

Il server divide lo spazio con documenti cartacei a sufficiente distanza di sicurezza.

Programmi applicativi

Sono in dotazione alla scuola: Office XP Professional; Argo: alunni, bilancio, libri di testo, magazzino, personale, protocollo, stipendi, fisco; PDF

Tutti i programmi software applicativi sono coperti da contratto di manutenzione (migliorativa, correttiva) e assistenza tecnica.

5. Criteri per l'individuazione dei rischi e la loro valutazione

8.1. Criteri per l'individuazione dei rischi

Per garantire la disponibilità, l'integrità, l'autenticità e la riservatezza delle informazioni, gli articoli da 33 a 36 del Testo Unico in materia di Trattamento dei dati personali di cui al D.Lgs. 30 giugno 2003 n. 196 prevedono l'obbligo di adottare misure minime di sicurezza, ai sensi dell'allegato B del disciplinare tecnico del Testo Unico, che possono essere individuate sulle base di tre grandi categorie di rischi:

- rischi connessi ad eventi relativi al contesto fisico ambientale;
- rischi connessi al mancato rispetto da parte degli operatori degli adempimenti e delle prescrizioni statuite sulla base del disposto Testo Unico in materia di trattamento di dati personali;
- rischi propri del sistema informatico utilizzato dall'Istituto Scolastico.

L'analisi dei possibili rischi è stata, pertanto suddivisa in tre settori di rischio nettamente differenti e separati per tipologia e materia.

A- Eventi relativi al contesto fisico – ambientale

In questo settore sono stati identificati e valutati i rischi legati ad eventi incontrollabili o astrattamente preventivabili di origine fortuita, dolosa o colposa (es. legati alla eventualità che persone non autorizzate possano accedere nei locali) e sono riferiti al luogo dove gli strumenti sono ubicati e quindi agli archivi esistenti negli uffici, agli elaboratori in rete ed ai server ivi ubicati.

Fonti di rischio	Rischio
1. Accessi non autorizzati a locali ad accesso ristretto	– Dispersione, perdita o alterazione, anche irreversibile, di dati; – visione abusiva di dati, furto di documenti, uso non autorizzato dei dati; – manomissione di programmi e di elaboratori; – impossibilità temporanea di accesso ai dati e di utilizzo dei programmi.

2. Asportazione e furto di strumenti contenenti dati	– Dispersione e perdita di dati, di programmi e di elaboratori; – accesso altrui non autorizzato
3. Movimenti tellurici, scariche atmosferiche, incendi, allagamenti, eventi distruttivi dolosi, accidentali o dovuti ad incuria o vandalismo	– Perdita di dati, dei programmi e degli elaboratori
4. Guasti a impianto elettrico, climatizzazione, etc.	– Perdita o alterazione, anche irreversibile, di dati; – manomissione dei programmi e degli elaboratori; – impossibilità temporanea di accesso ai dati e di utilizzo dei programmi

B. Comportamento degli operatori

In questo primo settore sono stati identificati e valutati i rischi legati all'attività delle persone (docenti ed ATA) incaricate del trattamento dei dati.

Fonti di rischio	Rischio
1. Mancato rispetto del divieto di accesso agli archivi fisici o informatizzati non autorizzati	– Sottrazione / presa visione / copia abusiva di informazioni e dati; – potenziale diffusione di dati anche quando non intenzionale (es. cestinare un semplice documento cartaceo senza provvedere alla sua distruzione); – distruzione / alterazione di dati.
2. Mancata custodia, anche temporanea, dei documenti estratti dall'archivio	
3. Mancata custodia, anche temporanea, della propria postazione informatica, una volta resa accessibile con le proprie credenziali di autenticazione	
4. Mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio	
5. Mancata distruzione dei supporti raggiunta la finalità	
6. Mancata conservazione o restituzione dei documenti cartacei	– Cancellazione anche accidentale di dati e conseguente loro perdita; – alterazione di dati; – trattamento illegittimo di dati per loro comunicazione a soggetti non autorizzati; – trattamento non conforme alle finalità della raccolta; – comunicazioni/diffusione di dati personali non previste preventivamente dalla legge
7. Comportamenti imprevisti, imprudenti o negligenti, errori materiali dei soggetti legittimati al trattamento dei dati	
8. Comportamenti dolosi dei soggetti legittimati	

C. Eventi relativi agli strumenti

In questo settore sono stati identificati e valutati i rischi legati alle infrastrutture tecnologiche (risorse hardware e software) e il rischio di intrusione nelle reti di comunicazione durante la normale attività del sistema informatico. Tali rischi sono collegati a :

- tasso di obsolescenza delle apparecchiature,
- modalità di esecuzione delle copie di sicurezza,
- funzionalità di accesso,
- quote disco condivise in lettura,
- rete di comunicazione accessibile al pubblico,
- utilizzo di periferiche di input.

Fonti di rischio	Rischio
1. Azione di virus informatici con conseguente danno HW e/o SW	– Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori.
2. Alterazione HW e SW a causa di sabotaggio	– Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; – impossibilità temporanea di accesso ai dati e di utilizzo dei programmi.
3. Alterazione o distruzione di dati a causa di sabotaggio	
4. Malfunzionamento, indisponibilità o degrado degli strumenti HW	
5. Malfunzionamento SW	
6. Guasto Tecnologico	
7. Accessi esterni non autorizzati	– Presa visione, copia abusiva, sottrazione di dati; – perdita o alterazione, anche irreversibile, di dati; – uso non autorizzato di applicativi; – manomissione di programmi e di elaboratori; – impossibilità temporanea di accesso ai dati e di utilizzo dei programmi.
8. Perdita delle copie di back-up	– Presa visione, copia abusiva, – perdita, anche irreversibile, di dati;
9. Perdita o riutilizzo non autorizzato di supporti magnetici	
10. Intercettazione delle trasmissioni di dati	– Diffusione di dati.

5.1. Criteri per la valutazione dei rischi

Una volta individuati i rischi, per procedere alla loro valutazione è necessaria una indicizzazione delle possibili perdite tenendo in considerazione due fattori:

- **probabilità (P) di accadimento**, che riguarda la frequenza riscontrata o riscontrabile:

		Probabilità
1	Non sono noti episodi.	IMPROBABILE
2	Sono noti rarissimi episodi.	POCO PROBABILE
3	Noto qualche episodio in cui la mancanza rilevata ha fatto seguito a un danno.	PROBABILE
4	Si sono verificati danni per la stessa mancanza rilevata in situazioni simili.	ALTAMENTE PROBABILE

- **magnitudo (M) delle conseguenze** nel caso l'evento si verifichi. In effetti la valutazione del rischio nel trattamento del dato deve tener conto sia della sua importanza che del danno legato al diritto che verrebbe ad essere leso.

  Dobbiamo quindi distinguere diverse tipologie di dati
  - dati conoscibili da chiunque,
  - dati accessibili ai sensi della legge 241/90,
  - dati sensibili e giudiziari

  a cui corrisponde diverso grado di rischio intrinseco connesso alla loro perdita, alterazione, comunicazione o diffusione perché:

- idonei a rivelare informazioni di carattere sensibile o giudiziario dei soggetti interessati, che sono quindi accomunati dall'elevato grado di pericolosità per la privacy dei soggetti interessati,
- costituiscono una importante risorsa, funzionale e tecnologica, per il Titolare, in relazione ai danni che conseguirebbero da una eventuale loro perdita.

Ne conseguono i seguenti criteri:

			Magnitudo
1	Perdita dei dati	diritto alla protezione	BASSA
2	Alterazione dei dati	diritto all'identità personale	MEDIA
3	Trattamento illecito/diffusione/comunicazione di dati personali	diritto alla riservatezza	MEDIO - ALTA
4	Trattamento illecito/diffusione/comunicazione di dati sensibili	diritto alla riservatezza	ALTA

Il Rischio (R) è la risultante della probabilità e della gravità di un evento: **R = P x M**

Dando a **P** e a **M** un valore fra 1 e 4, si ottiene un valore **R** compreso fra 1 e 16.

6. Individuazione e valutazione dei rischi

Si è proceduto all'individuazione dei rischi utilizzando le apposite matrici, in cui sono riportati i singoli fattori di rischio divisi sulla base dei possibili accadimenti relativi a:

- contesto fisico-ambientale (**Tavola 1**);
- comportamento degli operatori (**Tavola 2**);
- sistema informatico utilizzato dall'Istituto Scolastico (**Tavola 3**).

Nell'analisi dei rischi, questi sono stati valutati astrattamente, cioè a prescindere dalle misure che sono state già adottate, per facilitare sia la verifica dell'idoneità e l'efficacia delle misure stesse che la valutazione degli interventi adeguativi necessari.

Le tavole di valutazione del rischio riportano:
- fonte di rischio,
- magnitudo del rischio,
- probabilità del rischio,
- rischio calcolato.

7. Misure di protezione necessarie in relazione al contesto descritto

Dopo aver analizzato e valutato i fattori di rischio di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta, vanno individuate le misure di prevenzione e protezione più idonee a:

- eliminare il rischio,
- prevenire il rischio per diminuire la probabilità di accadimento;
- contenere l'impatto di un evento dannoso e diminuire la gravità degli effetti causati eventualmente dall'accadimento ;
- trasferire le conseguenze patrimoniali dell'evento (es. stipula contratto di assicurazione).

Nell'individuazione di tali misure sono presi in considerazione i seguenti aspetti:

- leggi, raccomandazioni e normative;
- sicurezza fisica e logica;
- definizione di ruoli, incarichi, procedure e formazione del personale;
- costi in relazione agli obiettivi e alle risorse disponibili.

Le matrici (**Tavole 1, 2, 3**), in cui sono riportati i singoli fattori di rischio registrano anche:

- le misure ritenute idonee per eliminarli, prevenirli, contenere o trasferire il rischio,

- le misure in essere al momento in cui viene effettuata la valutazione dei rischi,
- le misure che devono essere adottate e il termine entro cui le stesse vanno assunte.

7.1. Misure fisiche

	Rischio	Misure di protezione	
01	Sottrazione / presa visione / copia abusiva di informazioni e dati conseguente a - accessi non autorizzati a locali ad accesso ristretto; - asportazione e furto di strumenti contenenti dati.	Vigilanza della sede	- Chiusura a chiave locali - Sistemi di allarme - Cartelli segnaletici di divieto di accesso
		Custodia e archiviazione di atti, documenti e supporti	- Chiusura a chiave locali e armadi - Procedura gestione chiavi - Autenticazione accessi - Custodia in armadi ignifughi - Custodia in armadi blindati
02	Perdita di dati dovuta a - movimenti tellurici, scariche atmosferiche, incendi, allagamenti, eventi distruttivi dolosi, accidentali o dovuti ad incuria o vandalismo - guasti a impianto elettrico, gruppo di continuità, climatizzazione, etc.	Adeguamento e manutenzione strutture ed impianti	- Impianto elettrico a norma - Sistemi di protezione antincendio - Costruzione antisismica - Impianto di messa a terra - PC sollevati da terra per proteggerli in caso di allagamento

Alle misure individuate devono accompagnarsi quelle di natura organizzativa che riguardano:

- l'assegnazione di incarichi, autorizzazioni e compiti al personale dipendente;
- le istruzioni operative agli incaricati per il servizio di sorveglianza, la custodia e l'archiviazione di atti, documenti e supporti, le modalità di accesso, il controllo delle presenze di personale e alunni;
- la definizione di procedure per i controlli fisici all'accesso, la gestione delle chiavi, il carico/scarico di documenti, la manutenzione degli impianti e dei locali.

Particolare attenzione è prestata per gli archivi e i documenti relativi a dati sensibili e giudiziari affinché ai dati non possano accedere persone prive di autorizzazione.

7.2. Misure organizzative

Individuati e valutati tutte le fonti di rischio e i rischi annessi, sulla base dell'analisi del flusso dei dati e dei soggetti ai quali vengono comunicati, sono stati determinati i seguenti provvedimenti :

- individuazione dei responsabili e degli incaricati al trattamento (**Allegato C**);
- istruzioni operative per il personale con misure graduate per classi di dati (**Allegato B**).

	Rischio	Misure di protezione	
01	Perdita o alterazione di dati dovuta a - mancata conservazione o restituzione dei documenti cartacei; - ad errori materiali o a comportamenti imprudenti o negligenti;	Istruzioni operative Controlli periodici	- Istruzioni organizzative e tecniche;

02	Diffusione di dati causata da - mancata custodia dei documenti o della propria postazione, - mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio, - mancata distruzione dei supporti raggiunta la finalità		- Istruzioni organizzative e tecniche sui comportamenti da tenere; - sorveglianza sulla distruzione dei supporti rimovibili; - presenza in segreteria di appositi distruggi documenti cartacei;
03	Trattamento non conforme o illegittimo di dati e loro comunicazione o diffusione a soggetti non autorizzati	Assegnazione e incarichi Istruzioni operative Controlli periodici	- Adozione di procedure riguardo a soggetti e modalità con cui i dati possono essere comunicati dalla segreteria scolastica verso l'esterno
04	Sottrazione / presa visione / copia abusiva di informazioni e dati conseguente al mancato rispetto del divieto di accesso agli archivi fisici o informatizzati non autorizzati.	Log file Ingresso controllato	- Organizzazione servizio di sorveglianza - Credenziali di accesso - Consultazioni registrate - Controllo fotocopiatura (Fotocopiatrice con password e registrazione numero copie)

Si ritiene infine che solo un'adeguata conoscenza del disposto normativo può realmente e proficuamente garantire l'osservanza del medesimo ed, in definitiva, abbattere i rischi connessi a questo settore che è sicuramente il più rilevante e quindi quello a cui vanno dedicate le maggiori attenzioni per garantire un trattamento dei dati conforme alle prescrizioni legislative.

7.3. Misure logiche

Per i trattamenti effettuati con strumenti elettronici (elaboratori, programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato), è stato predisposto uno specifico **Disciplinare tecnico** con le norme di comportamento da tenere (**Allegato B**) per evitare:

- i rischi di intrusione,
- la diffusione illegittima di dati,
- l'accesso abusivo.

	Rischio	Misure di protezione	
01	Perdita o alterazione di dati / applicativi dovuta a - azione di virus informatici con conseguente danno HW e/o SW; - alterazione HW e SW a causa di sabotaggio; - malfunzionamento, indisponibilità o degrado degli strumenti HW o SW; - perdita delle copie di back-up; - disponibilità di periferiche di input	Disciplinare tecnico Contratti di assistenza tecnica applicativa e sistemistica Servizi di manutenzione correttiva e straordinaria dei programmi	- Firewall antintrusione come modulo software; - servizio di filtraggio antivirus e antispamming per il controllo dei messaggi e degli allegati di posta elettronica, - controllo delle pagine Internet in ordine a cookies, activex, java; - controllo antivirus in automatico di ogni file scaricato dalla rete o letto da supporti esterni quali Floppy Disk e CD-ROM; - aggiornamento automatico con frequenza oraria dell'antivirus; - back-up dei programmi applicativi - back-up periodico - deposito delle copie di sicurezza in armadio dislocato nell'ufficio del dsga

02	Diffusione di dati causata da intercettazione delle trasmissioni		- Ricorso a tecniche di crittografia per assicurare la riservatezza; - ricorso a tecniche in grado di assicurare la non modificabilità delle informazioni durante la trasmissione; - meccanismi di notifica di ricezione per verificare il non ripudio da parte del destinatario;
03	Sottrazione / presa visione / copia abusiva di informazioni e dati conseguente ad accessi non autorizzati.		Separazione sistema server di dati e di applicazioni dell'Istituto dal router ADSL per l'accesso ad Internet; - identificazione utente; - autenticazione utente; - credenziali di accesso; - definizione quote disco condivise in lettura; - controllo accessi; - registrazione accessi

L'accesso al sistema informatico è consentito a sole persone autorizzate ed è previsto un registro di controllo delle presenze.

E' utilizzato un software antivirus, in grado di riconoscere virus polimorfici, per il controllo delle attività sul Personal Computer, dei messaggi di posta elettronica, degli allegati di posta elettronica, delle pagine Internet. Il sistema è centralizzato e aggiorna i server e le postazioni con frequenza giornaliera.

Il sistema antivirus è di tipo centralizzato

La posta internet è gestita da Net Line e Namirial spa, quella intranet dal MIUR.

L'antivirus controlla in automatico ogni file scaricato dalla rete o letto da supporti esterni quali Floppy Disk, CD-ROM e chiavette ed è possibile programmare un controllo approfondito periodico di tutti i file presenti nel sistema.

Il personale ha ricevuto le necessarie istruzioni al fine di evitare l'introduzione di virus informatici nella rete.

L'accesso ad Internet è consentito utilizzando la rete LAN mediante un unico punto (router ADSL) separato e distinto dal sistema server di dati e di applicazioni dell'Istituto.

7.4. Misure di sicurezza suppletive relative al trattamento di particolari dati sensibili

In caso di trattamento di dati sensibili o giudiziari (punto 19.8 del D.Lgs. n. 196/2003) ed in particolare per i dati personali idonei a rivelare lo stato di salute, devono essere adottati particolari accorgimenti:

1. la custodia / archiviazione di tali dati separatamente dagli altri dati personali dell'interessato;
2. l'accesso, per la consultazione e/o modificazione, condizionato dal rispetto della procedura di identificazione per cui:
   a. l'incaricato deve essere precisamente individuato ed autenticato;
   b. l'incaricato può trattare i dati sensibili solo con un appropriato profilo di autorizzazione;
   c. l'incaricato deve essere in possesso della chiave di accesso.

   I dati sensibili debbono essere nettamente separati e gestiti autonomamente ed indipendentemente da ogni incaricato unicamente in base al proprio profilo di autorizzazione e per quel che attiene i dati personali degli alunni riportati sul registri didattici va prevista apposita procedura per la loro raccolta e custodia;
3. la protezione crittografica per la trasmissione di dati.

7.5. Programma delle misure

Il programma delle misure di sicurezza adottate o da adottare per ogni categoria di rischi è sistematicamente aggiornato nell'ottica di un miglioramento continuo del Sistema Sicurezza dell'Istituto Scolastico con cadenza annuale e in tutte le occasioni in cui si riscontri necessità di intervento o non conformità (tecniche o normative).

Il criterio adottato dall'Istituto per stabilire uno scadenzario degli interventi considera il tempo, espresso in mesi, in funzione inversa all'indice **R** di gravità:

R = 16 intervento entro 01 mesi e verifica entro 10 giorni

R = 12 intervento entro 04 mesi e verifica entro 20 giorni

R = 08 intervento entro 08 mesi e verifica entro 30 giorni

R = 04 intervento entro 12 mesi e verifica entro 40 giorni

R = 01 intervento entro 16 mesi e verifica entro 60 giorni.

Il programma delle misure di protezione necessarie per il trattamento dei rischi analizzati e valutati è riportato nelle tavole di valutazione dei rischi assieme alla definizione dei tempi previsti per la loro adozione.

Sono state previste anche le modalità e approntati gli strumenti di rilevazione per la verifica dell'effettiva adozione delle misure programmate e per il monitoraggio dell'idoneità delle stesse (REGISTRI: 04.06, 04.12, 04.13, 04.14, 04.15, 04.16).

7.6. Affidamento dei dati a soggetti esterni

Per la generalità dei casi, in cui il trattamento di dati personali, **di qualsiasi natura**, venga affidato all'esterno della struttura del titolare, sono impartite istruzioni per iscritto al terzo destinatario

Nei casi in cui ciò si renda opportuno, per ragioni operative legate anche alla tutela dei dati personali, il destinatario esterno viene nominato dal Titolare come responsabile del trattamento dei dati, mediante apposita lettera scritta.

8. Formazione del personale

La previsione di interventi formativi degli incaricati del trattamento rientra tra gli aspetti più importanti del presente documento.

In effetti, una gestione impropria da parte del personale ATA chiamato alla gestione dei dati personali nonché del corpo insegnante per quel che attiene il trattamento dei dati degli alunni effettuato con i registri di classe, la mancanza di chiare direttive esplicative e l'assenza di strumenti di controllo di facile e rapida applicazione costituiscono le cause principali del verificarsi, anche inconsapevole, di danni agli interessati ed in definitiva la causa prioritaria di trattamenti illegittimi e non conformi alle specifiche finalità dell'istituzione scolastica.

Gli interventi formativi sono programmati in modo da avere luogo al verificarsi di una delle seguenti circostanze:

- al momento dell'ingresso in servizio;
- in occasione di un cambiamenti di mansioni che implichi modifiche rilevanti rispetto al trattamento di dati personali;
- in occasione della introduzione di nuovi significativi strumenti con conseguenti rilevanti modifiche nel trattamento di dati personali.

8.1. Scopo della formazione

Il D. Lgs. 196/2003 impone la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare.

Di conseguenza l'Istituto interventi formativi degli incaricati del trattamento, finalizzati a renderli edotti dei seguenti aspetti:

- profili della disciplina sulla protezione dei dati personali, che appaiono più rilevanti per l'attività svolta dagli incaricati, e delle conseguenti responsabilità che ne derivano;
- rischi che incombono sui dati
- misure disponibili per prevenire eventi dannosi e procedure da seguire;
- modalità per mantenersi aggiornati sulle misure di sicurezza adottate dal titolare.

8.2. Modalità di formazione degli incaricati del trattamento dei dati personali

Sotto la diretta vigilanza e il coordinamento del Responsabile del Trattamento è prevista la predisposizione e l'applicazione di un adeguato e dettagliato piano di formazione del personale che contempla la possibilità di:

- AGGIORNAMENTO PERIODICO sotto la diretta vigilanza del Responsabile del Trattamento con cadenza almeno annuale stabilito in coincidenza con l'obbligo di aggiornamento del Documento Programmatico sulla Sicurezza;
- AGGIORNAMENTO SPECIFICO, tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuove banche dati oppure utilizzi nuovi strumenti informatici e/o nuove e diverse procedure mediante un programma individuale che deve essere impartito dal Responsabile in relazione alla nuova e specifica attività di trattamento svolta.

Gli interventi formativi possono avvenire:

- mediante la consegna di materiale esplicativo riguardante le norme, gli adempimenti richiesti nonché le misure minime di sicurezza applicate dall'Istituto;
- all'interno dell'Istituto, a cura del responsabile per la sicurezza, del responsabile al trattamento o di altri soggetti esperti nella materia,
- all'esterno dell'istituto, presso soggetti specializzati.

8.3. Valutazione dell'efficienza del piano di formazione

Il Responsabile del Trattamento dei dati personali, dopo avere dettagliatamente individuato il contenuto del piano di formazione del personale ATA e degli insegnanti, approntа una serie di strumenti di verifica dell'efficienza della formazione impartita per essere certo che essa sia stata realmente recepita dagli incaricati del trattamento e che sia stata funzionale ad un appropriato e sicuro trattamento dei dati personali.

9. Ripristino dei dati

Le misure ritenute idonee per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni[1] sono:

1. residenza dei dati in una struttura documentale sul server condivisa in rete e non sui dischi dei singoli P.C.;
2. procedure automatiche di backup dei database e dei dati contenuti nel server su supporti adeguati alla quantità di dati che deve essere salvata;
3. copie di back-up giornaliere su hard disk per le banche dati gestionali e istruzioni organizzative e tecniche che prevedono il salvataggio con frequenza almeno settimanale per quanto riguarda la gestione documentale;
4. etichettatura ed archiviazione dei supporti utilizzati per il backup dei dati con conservazione delle copie di sicurezza in cassaforte;
5. procedure di recupero immediato dei dati in caso di attacchi;
6. analisi e test di tutti i software in possesso dell'Istituto scolastico di tutti gli hardware nonché tutti gli altri strumenti informatici tecnico-operativi dell'intero sistema informatico scolastico.

Sono salvati anche i sistemi attraverso la copia della configurazione di sistema/rete su hard disk di backup e copie del sistema operativo e degli applicativi presenti nei server, tramite backup su hard disk e CD affinché siano ripristinabili. Si provvede al rifacimento di tali copie con periodicità dettata dagli interventi di manutenzione e aggiornamento del software di base (sistemi operativi, piattaforme database, ecc.) e dei programmi applicativi.

Per quanto riguarda i documenti cartacei e i supporti diversi da quelli elettronici contenenti dati personali, essi sono fascicolati e depositati:

- presso l'archivio generale per quanto riguarda gli ex studenti e il personale non più in servizio
- nell'archivio corrente per quanto riguarda gli studenti e il personale in servizio

[1] La legge sul protocollo, superando la norma del codice, richiede che il sistema sia recuperabile in esercizio entro 24 ore.

10. Attività di controllo e valutazione

Al fine di verificare l'efficacia delle misure di sicurezza adottate, il responsabile del trattamento e le persone da questo appositamente incaricate provvedono, in modo estemporaneo, anche con verifiche casuali e non annunciate e/o con controlli a campione, a verificare che le misure implementate, sia quelle tecnologiche che quelle organizzative, siano effettivamente applicate e svolgano correttamente le funzionalità per cui sono state adottate.

Tale verifica si sostanzia nelle seguenti attività:

- verificare l'accesso fisico ai locali dove si svolge il trattamento
- verificare la correttezza delle procedure di archiviazione e custodia di atti, documenti e supporti contenenti dati personali;
- monitorare l'efficacia ed il corretto utilizzo delle misure di sicurezza adottate per gli strumenti elettronici;
- verificare l'integrità dei dati e delle loro copie di backup;
- verificare la sicurezza delle trasmissioni in rete;
- verificare che i supporti magnetici, che non possono più essere riutilizzati, vengano distrutti;
- verificare il livello di formazione degli incaricati.

Almeno ogni sei mesi, si procede ad una sistematica verifica del corretto utilizzo delle parole chiave e dei profili di autorizzazione che consentono l'accesso agli strumenti elettronici da parte degli incaricati, anche al fine di disabilitare quelli che non sono stati mai utilizzati in sei mesi.

Mediante l'analisi dei log file adottando strumenti automatici di reportistica e di sintesi, nei quali i software di sicurezza installati, i sistemi operativi e le applicazioni scrivono le operazioni svolte dagli incaricati per il loro tramite, è possibile individuare i tentativi, riusciti o meno, di accesso al sistema e l'esecuzione di operazioni non corrette, o sospette.

Delle attività di verifica svolte viene redatto apposito verbale, che viene conservato dal Titolare del trattamento.

In sede di valutazione il Titolare del trattamento, coadiuvato dal Responsabile del trattamento e dall'Amministratore di sistema, analizza l'efficacia degli strumenti adottati al fine di

- rivedere se necessario l'indice di gravità dei rischi controllando quali danni si sono avuti o quali siano possibili, la frequenza degli accadimenti registrati, le circostanze in cui si sono subiti attacchi;
- individuare le misure che sono risultate non adeguate e che vanno riconsiderate.

Al responsabile del trattamento è affidato il compito di aggiornare le misure di sicurezza, al fine di adottare gli strumenti e le conoscenze, resi disponibili dal progresso tecnico, che consentano di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito.

A tale fine, è previsto che al Responsabile venga affidato un budget annuo che può utilizzare in autonomia, nel rispetto delle normative di legge e di regolamento relative alle forniture pubbliche.

Il presente documento, redatto il giorno 30 del mese di marzo dell'anno 2011, è stato assunto al protocollo dell'Istituto in data 30 marzo 20011 col numero 1775/A32.

L'originale del presente documento viene custodito presso l'Amministrazione Scolastica, per essere esibito in caso di controlli.

Vittorio Veneto, 30 marzo 2011

IL TITOLARE DEL TRATTAMENTO

Prof.ssa Franca Braido

TAVOLA 1

Fonti di rischio collegate al contesto fisico-ambientale:

1. Accessi non autorizzati a locali ad accesso ristretto e conseguenti possibilità di furto, sabotaggio, presa visione abusiva atti, furto di documento, uso non autorizzato dei dati.
2. Furto di strumenti informatici contenenti dati.
3. Movimenti tellurici, scariche atmosferiche, incendi, allagamenti, eventi distruttivi dolosi, accidentali o dovuti ad incuria o vandalismo.
4. Guasti a impianto elettrico, gruppo di continuità, climatizzazione, etc.

	Fonte di rischio	M	P	R	Misure Idonee	Misure Adottate	Misure da Adottare …	… entro
1	Ingresso non controllato	3	2	3x2 = 6	Organizzazione servizio di sorveglianza Sistemi di allarme	Vigilanza Sistema di allarme ala nuova dell'edificio	Sistema di allarme ala vecchia dell'edificio da parte dell'Ente Provincia	12 mesi
2	Ingresso non autorizzato	2	2	2x2 = 4	Istruzioni operative per servizio di sorveglianza Controllo presenze personale e alunni	Registro controllo presenze del personale e degli alunni		
3	Accesso non autorizzato archivi dati comuni	2	2	2x2 = 4	Assegnazione incarichi Chiusura a chiave locali e armadi Procedura gestione chiavi Cartelli segnaletici di divieto di accesso	Chiusura a chiave Assegnazione incarico	Procedura gestione chiavi Cartelli segnaletici	12 mesi
4	Accesso non autorizzato archivi dati sensibili o giudiziari	4	2	4x2 = 8	Assegnazione incarichi Chiusura a chiave locali e armadi Casseforti Procedura gestione chiavi Procedura carico/scarico documenti Istruzioni operative	Assegnazione incarico	Procedura gestione chiavi	12 mesi
5	Fotocopie abusive	2	2	2x2 = 4	Fotocopiatrice con password Registrazione numero copie	Assegnazione password Registrazione copie		
6	Furto HW	2	1	2x1 = 2	Chiusura a chiave locali	Chiusura a chiave locali		

					Sistemi di allarme Back-up	Sistema di allarme Back-up giornaliero		
7	Furto o copiatura SW	2	1	2x1 = 2	Credenziali di accesso Back-up Log file (solosul bak-up deiserver)	Password di accesso Back-up Log file sul bak-up del server		
8	Incendio	3	2	3x2 = 6	Sistemi di protezione antincendio Piano di emergenza Back-up	Sistema antincendio Piano di emergenza Back-up		
9	Allagamento	2	2	2x2 = 4	PC sollevati da terra Piano di emergenza Back-up	PC sollevati da terra Back-up		
10	Scariche atmosferiche	2	2	2x2 = 4	Impianto di messa a terra Regolare manutenzione Back-up	Impianto di messa a terra Regolare manutenzione Back-up		
11	Cedimento strutturale / Terremoto	3	2	3x2 = 6	Costruzione antisismica Piano di emergenza Back-up	Costruzione antisismica Piano di emergenza Back-up		
12	Cortocircuito	1	2	1x2 = 2	Impianto certificato	Impianto certificato		
13	Mancanza di alimentazione elettrica	1	3	1x3 = 3	Gruppo di continuità Back-up	Back-up		

TAVOLA 2

Fonti di rischio collegate al comportamento degli operatori:

1. possono venire sottratte o cedute le credenziali di autenticazione con conseguente accesso a dati per cui non esiste autorizzazione;
2. i soggetti legittimati al trattamento dei dati possono mettere in atto comportamenti imprevisti, imprudenti o negligenti o errori materiali che danneggiano i dati o ne consentono la loro comunicazione e/o diffusione;
3. i soggetti legittimati possono mettere in atto comportamenti dolosi per manomettere o acquisire informazioni custodite dall'Istituto.

	Fonte di rischio	M	P	R	Misure Idonee	Misure Adottate	Misure da Adottare…	… entro
1	Assenza del personale incaricato	1	3	1x3 = 3	Gestione risorse umane Formazione	Gestione risorse umane		
2	Mancato rispetto del divieto di accesso agli archivi fisici o informatizzati non autorizzati e conseguente sottrazione / presa visione abusiva di informazioni e dati	3	1	3x1 = 3	Credenziali di accesso Istruzioni operative Sanzioni disciplinari Log file	Password di accesso Istruzioni operative Sanzioni disciplinari Log file		
3	Cancellazione di dati e conseguente loro perdita	1	2	1x2 = 2	Credenziali di accesso Back-up Istruzioni operative Log file Sanzioni disciplinari	Password di accesso Back-up Istruzioni operative Log file Sanzioni disciplinari		
4	Alterazione di dati	2	2	2x2 = 4	Credenziali di accesso Back-up Istruzioni operative Log file Sanzioni disciplinari	Password di accesso Back-up Istruzioni operative Log file Sanzioni disciplinari		
4	Comunicazione/diffusione illegale dei dati e dei documenti	3	1	3x1 = 3	Credenziali di accesso Istruzioni operative Controllo fotocopiatura Sanzioni disciplinari	Password di accesso Istruzioni operative Registro copie Sanzioni disciplinari		
5	Mancata custodia, anche temporanea, dei documenti estratti dall'archivio o della postazione informatica quando "accessibile"	3	2	3x2 = 6	Istruzioni operative Verifiche Sanzioni disciplinari	Istruzioni operative Verifiche Sanzioni disciplinari		

6	Mancata custodia, anche temporanea, della propria postazione una volta connessi al sistema con le proprie credenziali di autenticazione	3	2	3x2 = 6	Istruzioni operative Verifiche Sanzioni disciplinari	Istruzioni operative Verifiche Sanzioni disciplinari		
7	Mancata conservazione o restituzione dei documenti cartacei	2	1	2x1 = 2	Istruzioni operative Verifiche Sanzioni disciplinari	Istruzioni operative Verifiche Sanzioni disciplinari		
8	Mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio	3	2	3x2 = 6	Istruzioni operative Verifiche Sanzioni disciplinari	Istruzioni operative Verifiche Sanzioni disciplinari		
9	Perdita, mancata distruzione o riutilizzo non autorizzato dei supporti raggiunta la finalità	3	2	3x2 = 6	Istruzioni operative Verifiche Sanzioni disciplinari	Istruzioni operative Verifiche Sanzioni disciplinari		
10	Mancata custodia, anche temporanea, dei documenti contenenti dati sensibili o giudiziari estratti dall'archivio	4	2	4x2 = 8	Istruzioni operative Verifiche Sanzioni disciplinari	Istruzioni operative Verifiche Sanzioni disciplinari		
11	Mancata chiusura dei contenitori, degli armadi e dei locali adibiti ad archivio per i documenti contenenti dati sensibili o giudiziari	4	2	4x2 = 8	Istruzioni operative Verifiche Sanzioni disciplinari	Istruzioni operative Verifiche Sanzioni disciplinari		
12	Perdita, mancata distruzione o riutilizzo non autorizzato dei supporti contenenti dati sensibili o giudiziari raggiunta la finalità	4	2	4x2 = 8	Istruzioni operative Verifiche Sanzioni disciplinari	Istruzioni operative Verifiche Sanzioni disciplinari		
13								

TAVOLA 3

Fonti di rischio collegate al sistema informatico utilizzato dall'Istituto:

1. Azione di virus informatici o interventi di sabotaggio con conseguente perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori o impossibilità temporanea di accedere ai dati e di utilizzare i programmi.
2. Malfunzionamento, indisponibilità o degrado degli strumenti HW o SW.
3. Accessi esterni non autorizzati e conseguente presa visione, copia abusiva, sottrazione perdita o alterazione di dati, uso non autorizzato di applicativi o manomissione di programmi e di elaboratori.
4. Intercettazione di informazioni in rete e conseguente diffusione di dati.

	Fonte di rischio	M	P	R	Misure Idonee	Misure Adottate	Misure da Adottare …	… entro
1	Azione di virus informatici con conseguente danno HW e/o SW	4	4	4x4 = 16	Antivirus aggiornato Assistenza Back-up dei programmi applicativi Log file (solo sul back-up dei server)	Antivirus aggiornato Assistenza Back-up dei programmi applicativi Log file sul back-up del server		
2	Alterazione HW e SW a causa di sabotaggio	3	2	3x2 = 6	Custodia Assistenza Back-up periodico Log file (solo sul back-up dei server)	Chiusura a chiave dei locali Allarme Assistenza Back-up giornaliero Log file sul back-up del server		
3	Alterazione o distruzione di dati a causa di sabotaggio	2	2	2x2 = 4	Credenziali di accesso Firewall Back-up periodico Log file (solo sul back-up dei server)	Password di accesso Firewall Back-up giornaliero Log file sul back-up del server		
4	Perdita delle copie di back-up	4	1	4x1 = 4	Deposito delle copie di sicurezza in armadi dislocati presso …	Deposito delle copie di sicurezza in armadio blindato nell'ufficio del dsga		
5	Malfunzionamento, indisponibilità o degrado degli strumenti HW	1	2	1x2 = 2	Assistenza Back-up periodico	Assistenza Back-up giornaliero		

6	Malfunzionamento SW	1	2	1x2 = 2	Assistenza Back-up periodico	Assistenza Back-up		
7	Guasto Tecnologico	2	2	2x2 = 4	Manutenzione Back-up periodico Log file	Manutenzione Back-up giornaliero Log file		
9	Accessi esterni non autorizzati	3	2	3x1=2	Credenziali di accesso Firewall Registrazione accessi Back-up periodico Log file (solo sul bak-up dei server)	Password di accesso Firewall Back-up giornaliero Log file		
10	Intercettazione delle trasmissioni di dati	2	2	2x2 = 4	Crittografia Firma digitale Firewall Formazione personale Rapporti provider	Formazione personale	E' prevista l'acquisizione di dispositivi o software di controllo del traffico internet (PROXY SERVER) anche se trattasi di traffico limitato e già presidiato e l'acquisizione della funzione FIREWALL antiintrusione, o come dispositivo hardware o come modulo software nell'ambito del server LINUX.	