



**ISTITUTO TECNICO INDUSTRIALE  
“B. FOCACCIA “  
VIA MONTICELLI,1  
84100 SALERNO**

# **DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**

**Il presente DPSS è stato emesso il \_\_\_\_\_**

**con numero di Revisione n. 0 del =====**

**E' STATO REDATTO AI SENSI E PER GLI EFFETTI DELL'ARTICOLO 34, COMMA 1, LETTERA G) DEL DLGS 196/2003  
E DEL DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA”  
(ART. DA 33 A 36 DEL CODICE)ALLEGATO AL MEDESIMO DECRETO SUB B**



Il presente documento è finalizzato a delineare l'insieme delle misure di sicurezza, organizzative, fisiche, logistiche e logiche, da adottare per il trattamento dei dati personali effettuato dal seguente Titolare:

**ISTITUTO TECNICO INDUSTRIALE  
“B. FOCACCIA “  
VIA MONTICELLI,1  
84100 SALERNO**



## Indice degli argomenti

### Premessa

1. Elenco dei trattamenti di dati personali (regola 19.1)
2. Distribuzione dei compiti e delle Responsabilità (regola 19.2)
3. Analisi dei rischi che incombono sui dati (regola 19.3)
4. Misure in essere e da adottare (regola 19.4).
5. Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)
6. Formazione e pianificazione dei responsabili e degli incaricati al trattamento dei dati (regola 19.6)
7. Trattamenti affidati all'esterno (regola 19.7.)
8. Cifratura dei dati o separazione dei dati identificativi (regola 19.8) (regola 19.8)
9. Elenco dei luoghi in cui verranno trattati i dati
10. Elenco delle banche dati utilizzate dai diversi trattamenti
11. Elenco degli strumenti utilizzati nei diversi trattamenti

### Allegati al presente documento, di cui costituiscono parte integrante:

1. All. 1 : Descrizione analitica dei trattamenti di dati personali eseguiti in forma cartacea o elettronica
2. All. 5 : Descrizione delle procedure di sicurezza utilizzate
3. Informativa alunni/familiari
4. Informativa dipendenti/familiari
5. Informativa fornitori/clienti
6. Dichiarazione per Relazione annuale
7. Norme basilari di comportamento e regole operative
8. Regolamento interno per gli incaricati
9. Manutenzione ordinaria incaricati
10. Dicitura fax ed e-mail
11. Formula da inserire nei contratti per fornitori
12. Sintesi informativa sulla legge ad uso interno
13. Modello comunicazione password
14. Registri di verifica per RSI



### **Premessa**

Il Codice sulla privacy (D.lgs.vo 196/03) impone a chiunque tratta informazioni relative ad altre persone, imprese, enti od associazioni di rispettare alcuni principi fondamentali a garanzia della riservatezza dei dati stessi.

Il Codice prescrive precisi obblighi e comportamenti da attuare nel trattare dati; questi obblighi sono sanzionati anche penalmente: è necessario, pertanto, procedere all'adeguamento dell'organizzazione al fine di rispettare gli obblighi imposti dal Codice.

La finalità del “documento programmatico della sicurezza” è quella di definire i criteri e le procedure per garantire la sicurezza nel trattamento di dati personali.

Si rende noto che la rilevazione della stato di fatto è stata congelata alla data del **31 marzo 2011**. Eventuali cambiamenti che si dovessero rendere necessari saranno introdotti in questo DPSS indicando in copertina, le revisioni effettuate entro il 31 marzo, data entro la quale le citate disposizioni impongono la predisposizione e l'aggiornamento, con cadenza almeno annuale (entro il 31 marzo di ogni anno) di un Documento Programmatico sulla Sicurezza dei dati.

### **Validità del documento**

Il presente documento **è valido un anno**, si potranno aggiornare alcune informazioni qualora le stesse per motivi diversi non risultassero più coerenti con l'organizzazione o con il trattamento dei dati.

Inoltre le citate disposizioni impongono la predisposizione e l'aggiornamento, con cadenza almeno annuale (entro il 31 marzo di ogni anno) di un Documento Programmatico sulla Sicurezza dei dati.

#### **Il presente DPSS è stato redatto per :**

**Istituto Tecnico Industriale Statale "B. Focaccia"**  
**Sede Centrale in Via Monticelli 1**  
**84100 Salerno SA**  
**Cod. fiscale 80023050653**

#### **Con le seguenti sedi distaccate:**

**Sede via PIO X 84100 - Salerno (SA)**  
**Sede via Monticelli (Nuovi Edifici) - 84100 Salerno (SA)**  
**Sede Baronissi - Via Trinità – Località Sava (SA)**

N.	CLASSI	MASCHI	DONNE	Gruppo H	TOTALE
15	PRIME	332	39	9	380
16	SECONDE	279	41	4	324
15	TERZE	314	39	8	361
15	QUARTE	249	41	5	295
14	QUINTE	216	33	4	253
75	TUTTE	1468	193	30	1613



**Titolare del trattamento dei dati** a cui spetta la vigilanza sul rispetto da parte dei Responsabili e degli Incaricati delle proprie istruzioni nonché sulla puntuale osservanza delle disposizioni vigenti in materia di trattamento dei dati e loro sicurezza è la istituzione scolastica rappresentata dal Dirigente Scolastico – **Prof.ssa MARIA SAPONIERO**

(art. 28 D.Lgs. n° 196 del 30 giugno 2003).

**Definizioni:**

**Responsabile al trattamento dei dati:** Spetta il compito di promuovere lo sviluppo ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento Programmatico Sulla Sicurezza dei Dati Personali di seguito denominato DPSS; informare il titolare del trattamento sulle eventuali non corrispondenze con le norme di sicurezza e sugli eventuali incidenti; promuovere lo svolgimento di un continuo programma di addestramento degli incaricati al trattamento e mantenere attivo un programma di controllo, sorveglianza e monitoraggio della corrispondenza con le regole di sicurezza; promuovere e garantire l'esecuzione del programma di audit.

**Responsabile del sistema informativo –:** Spetta il compito di promuovere lo sviluppo ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento programmatico sulla sicurezza dei Dati Personali di seguito denominato DPS; informare il titolare del trattamento sulle eventuali non corrispondenze con le norme di sicurezza e sugli eventuali incidenti; promuovere lo svolgimento di un continuo programma di addestramento degli incaricati al trattamento e mantenere attivo un programma di controllo, sorveglianza e monitoraggio della corrispondenza con le regole di sicurezza; promuovere e garantire l'esecuzione del programma di audit. Garantire il funzionamento di tutti i dispositivi elettronici, degli strumenti, dei sistemi operativi, dei software, con particolare riferimento ai sistemi Antivirus, Firewall, al sistema di back-up, al sistema per il ripristino dei dati, alle reti, al controllo degli accessi.

**Incaricati al trattamento:** Nominati dal responsabile per iscritto devono svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente DPS e secondo le direttive del Responsabile al trattamento dei dati; rispettare e far rispettare le norme di sicurezza e le misure per la protezione dei dati personali; segnalare al responsabile eventuali anomalie o comportamenti pregiudizievoli sul trattamento dei dati; informare il responsabile in caso di incidente di sicurezza che coinvolga i dati personali;

**Incaricato al trattamento della custodia delle password:** Nominato dal responsabile per iscritto svolge le attività previste dal Responsabile alla gestione del sistema informatico; in particolare deve custodire in luogo sicuro ed a chiave le buste contenenti le password che gli perverranno dal/i Responsabile/i al trattamento dei dati, dal responsabile al Sistema Informatico e dagli incaricati al trattamento dei dati. In caso di necessità il responsabile al trattamento dei dati o il Responsabile al sistema informatico potrà richiedere la busta contenente una password, in tal caso il mittente della busta dovrà essere immediatamente avvertito affinché la possa sostituire consegnando all'incaricato alla custodia delle password la nuova busta contenente la nuova password. E' compito dell'incaricato verificare che vi siano le buste di tutti i responsabili e di tutti gli incaricati al trattamento dei dati comunicati dal/dai responsabile/i. L'incaricato alla custodia delle password deve rispettare e far rispettare le norme di sicurezza e le misure per la protezione dei dati personali; segnalare al responsabile eventuali anomalie o comportamenti pregiudizievoli sul trattamento dei dati; informare il responsabile in caso di incidente di sicurezza che coinvolga i dati personali;



**Strumenti:** Gli elaboratori, i programmi per elaboratori, qualunque dispositivo elettronico automatizzato o qualsiasi contenitore o mezzo impiegato per effettuare il trattamento dei dati

**Rischi:** Situazioni o comportamenti che possano generare un pericolo per i dati personali e/o sensibili. Per meglio valutare l'entità e le azioni da intraprendere il rischio prevede diversi livelli di soglia: lieve, medio, grave e gravissimo.

**Misure:** Il complesso delle misure cautelari tecniche, informatiche organizzative, logistiche e procedurali di sicurezza atti ad eliminare i rischi valutati e stimati nella progettazione della sicurezza in relazione alla soglia di gravità

**Profilo di autenticazione:** l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti

**Sistema di autorizzazione:** l'insieme degli strumenti e delle procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo di autorizzazione del richiedente

Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione (l'insieme degli strumenti elettronici, dei software e delle procedure atte a verificare l'identità) che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

1. Le credenziali di autenticazione (i dati ed i dispositivi, in possesso di una persona da questi conosciuti o ad essa univocamente correlati, utilizzati per l'autenticazione informatica) consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
2. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
3. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
4. E' un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per la protezione dei dati. Un corretto utilizzo ed impiego delle password è a garanzia dell'utente. Le regole di seguito elencate sono vincolanti per tutti i sistemi e le workstation (server, postazioni Pc client, portatili, ecc.) tramite le quali si può accedere alla rete o alle banche dati contenenti i dati personali. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. Non deve essere comunicata ad alcuno per alcun motivo, non deve essere conservata annotazione scritta in alcun posto specie nei pressi della postazione di lavoro.



5. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
6. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
7. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
8. Sono impartite le seguenti istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento. L'incaricato se si allontana dalla propria postazione dovrà mettere in protezione il suo sistema (Pc client o portatile) affinché persone non autorizzate non abbiano accesso ai dati protetti. La responsabilità sull'efficacia di tale sistema è assegnata al responsabile dei servizi informativi.
9. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite le seguenti idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema.

Per ogni PC si è stabilito a seconda del suo Sistema operativo la seguente procedura

Il responsabile del sistema informativo affida l'incarico al trattamento della custodia delle password ad un addetto. La responsabilità sull'efficacia di tale sistema è assegnata al responsabile del sistema informativo.

In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

Ogni utente dovrà obbligatoriamente consegnare in busta chiusa la propria password alla persona incaricata alla custodia delle chiavi di accesso che gli sarà indicata dal Responsabile al sistema informatico. In caso di necessità il responsabile al sistema informativo chiederà la busta contenente la password al custode per disporre della password di accesso al sistema. Al termine dei lavori comunicherà all'addetto della necessità di modificare la password. Per questo motivo ogni qualvolta per qualsiasi motivo un addetto modifica la sua password è **OBBLIGATO ALLA CONSEGNA IMMEDIATA DELLA BUSTA SIGILLATA CONTENENTE LA NUOVA PASSWORD AL CUSTODE**. La violazione di tale norma è grave e porta ad estreme conseguenze in quanto mette a repentaglio l'accesso ai dati da parte dell'organizzazione in caso di necessità. In tal caso i dati dovranno risiedere su di un server il cui accesso sarà limitato e vincolato al profilo della persona.

Se il sistema operativo non consente una gestione degli utenti differita tra amministratore del Pc ed utilizzatore si utilizzeranno profili differenti affinché sia sempre possibile l'accesso al PC in caso di necessità, di tale possibilità andrà avvisato l'utilizzatore.

Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.



### Sistema di autorizzazione

10. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
11. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
12. La normativa prevede che periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione, grazie ad un apposita check-list verrà redatto un verbale di verifica semestrale.

### Altre misure di sicurezza

Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

La normativa prevede che i dati personali debbano essere protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale grazie ad un apposita check-list verrà redatto un verbale di verifica semestrale.

Allo scopo un gateway deve essere protetto. E' definito Gateway l'insieme di hardware, software e applicazioni che permettono l'interconnessione (Internet) o l'accesso remoto a sistemi esterni. I Gateway devono consentire l'accesso alla rete interna solamente agli utenti autorizzati attraverso sistemi di controllo specifici (Proxy/Firewall). Pertanto tutte le cpu che sono collegate verso internet è necessario predisporre un sistema che impedisca accessi indesiderati. Tali sistemi anche se l'accesso è limitato nel tempo servono a prevenire l'accesso da parte di "intrusi" ai vostri sistemi di gestione dati. Tali sistemi sono denominati "Firewall". Tutti i vostri sistemi attraverso il server dati (se è quest'ultimo a consentire la connessione all'esterno) o direttamente per ogni singola cpu se ciascuno si connette ad internet con un modem deve disporne. Ogni trimestre è necessario verificare se sono disponibili degli aggiornamenti sul Firewall. La sottoscrizione di un servizio di notifica sugli aggiornamenti del prodotto sono consigliati. La responsabilità sull'efficacia di tale sistema è assegnata al responsabile dei servizi informativi. Le istruzioni riguardanti l'utilizzo del sistema FIREWALL e del relativo aggiornamento sono riportati nelle guide operative del prodotto.

La normativa prevede che gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti debbano essere effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari la normativa prevede che tale aggiornamento almeno a livello semestrale. I sistemi sensibili ai virus informatici (sistemi operativi, programmi informatici, data base) devono essere protetti con opportuni programmi antivirus che devono essere aggiornati per garantire la loro efficacia.

Trimestralmente dovrà essere verificato se il numero interno riportato da tutti i programmi antivirus è stato aggiornato al fine di verificare se il sistema di aggiornamento è funzionante grazie ad un apposita check-list verrà redatto un verbale di verifica semestrale. Resta facoltà degli interessati procedere con un controllo più frequente. In caso di mancato aggiornamento del software antivirus si dovrà provvedere a ripristinarne immediatamente il funzionamento. Le cpu che ricevono le mail direttamente dall'esterno dovranno disporre di un Antivirus in grado di



controllare le mail in arrivo e quelle in partenza, inoltre su tutte le cpu che contengono banche dati o se quelle che hanno accesso ad Internet dovrà essere condotto un controllo settimanale con evidenza oggettiva. In caso di segnali allarmanti (mail sospette, comportamenti della cpu imprevedibili) è necessario verificare immediatamente l'efficienza dell'antivirus ed il suo stato di aggiornamento. La responsabilità sull'efficacia di tale sistema è assegnata al responsabile dei servizi informativi. Le istruzioni riguardanti l'utilizzo del sistema antivirus e del relativo aggiornamento sono riportati nelle guide operative del prodotto.

Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale. **(vedi par. 5)**



1. Elenco dei trattamenti di dati personali (regola 19.1)

<b>Codice</b>	<b>Tr.1</b>			
<b>Nome del trattamento</b>	<b>Selezione e reclutamento a tempo indeterminato e determinato, gestione del rapporto di lavoro</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	I dati sono raccolti su iniziativa degli interessati o previa richiesta dell'Ufficio presso i medesimi interessati, ovvero presso altri soggetti pubblici o privati, e sono trattati, sia in forma cartacea che telematica, per l'applicazione dei vari istituti disciplinati dalla legge e dai regolamenti in materia di selezione, reclutamento, gestione giuridica, economica, previdenziale, pensionistica, aggiornamento e formazione del personale			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato, Ved. Regolamento Min. Pubblica Istruzione )</b>	<ul style="list-style-type: none"><li>○ Finalità di rilevante interesse pubblico perseguite</li><li>○ Norme relative al personale amministrativo del MIUR</li><li>○ Norme per il personale delle istituzioni scolastiche</li><li>○ Norme per il personale AFAM</li><li>○ Norme per il personale IRRE</li></ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>		<b>Elaborazione</b>	
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si



<p>Particolari forme di elaborazione</p>	<p><b><u>DIFFUSIONE : IN NESSUN CASO</u></b></p> <p><b><u>INTERCONNESSIONI E RAFFRONTI DI DATI CON ALTRO TITOLARE:</u></b></p> <ul style="list-style-type: none"><li>• Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000;</li></ul> <p><b><u>COMUNICAZIONE</u></b></p> <p><b><u>Solo ai seguenti soggetti per le seguenti finalità:</u></b></p> <ul style="list-style-type: none"><li>• <b>Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego;</b></li><li>• Organi preposti al riconoscimento della <b>causa di servizio/equo indennizzo</b>, ai sensi del D.P.R. n. 29 ottobre 2001, n. 461.( Regolamento recante semplificazione dei procedimenti per il riconoscimento della dipendenza delle infermita' da causa di servizio, per la concessione della pensione privilegiata ordinaria e dell'equo indennizzo, nonche' per il funzionamento e la composizione del comitato per le pensioni privilegiate ordinarie)</li><li>• Organi preposti alla <b>vigilanza in materia di igiene e sicurezza sui luoghi di lavoro</b> (d.lg. n. 626/1994 [non allegata perché comunque notissima]– norme in materia di prevenzione e sicurezza nei luoghi di lavoro.</li><li>• <b>Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza</b> a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o <b>infortuni sul lavoro</b> ai sensi del D.P.R. n. 1124/1965 (testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali).</li><li>• Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della Legge 12 marzo 1999, n. 68 (Norme per il diritto al lavoro dei disabili) Norme per il diritto al lavoro dei disabili</li><li>• <b>Organizzazioni sindacali</b> per gli adempimenti connessi al <b>versamento delle quote di iscrizione e per la gestione dei permessi sindacali;</b></li><li>• Pubbliche Amministrazioni presso <i>le</i> quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;</li><li>• <b>Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica</b> ai sensi della Legge 18 luglio 2003, n. 186 (Norme sullo stato giuridico degli insegnanti di religione cattolica degli istituti e delle scuole di ogni ordine e grado).</li><li>• <b>Organi di controllo</b> (Corte dei Conti e MEF): al fine del controllo di legittimità e annotazione della spesa <b>dei provvedimenti di stato giuridico ed economico del personale</b> ex Legge 14 gennaio 1994, n. 20 (Disposizioni in materia di giurisdizione e controllo della Corte dei Conti,) e D.P.R. 20 febbraio 1998, n. 38 (Regolamento recante le attribuzioni dei dipartimenti del ministero del tesoro, del bilancio e della programmazione economica, nonche' disposizioni in materia di organizzazione e di personale, a norma dell'articolo 7, comma 3, della legge 3 aprile 1997, n. 94)</li><li>• <b>Agenzia delle Entrate: ai fini degli obblighi fiscali del personale</b> ex:<ul style="list-style-type: none"><li>- Legge 30 dicembre 1991, n. 413 (disposizioni per ampliare le basi imponibili, per razionalizzare, facilitare e potenziare l'attività di accertamento; disposizioni per la valutazione obbligatoria dei beni immobili delle imprese, nonché per riformare il contenzioso e per la definizione agevolata dei rapporti tributari pendenti; delega al presidente della repubblica per la concessione di amnistia per reati tributari; istituzioni dei centri di assistenza fiscale e del conto fiscale);</li><li>- MEF e INPDAP: per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335 (Riforma del sistema pensionistico obbligatorio e complementare).</li></ul></li><li>• <b>Presidenza del Consiglio dei Ministri</b> per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art. 50, comma 3, D.Lgs.30 marzo 2001, n. 165 - Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.</li></ul>
--	---



Natura dei dati trattati	Comuni	Sensibili	Giudiziari
	Si	Si	Si
Struttura che concorre al trattamento	<ul style="list-style-type: none"><li>○ Dirigente Scolastico</li><li>○ Direttore amministrativo (DSG)</li><li>○ Segreteria Amministrativa e Assimilati</li></ul>		<ul style="list-style-type: none"><li>○ Collaboratori del D.S.,</li><li>○ Collaboratori scolastici,</li><li>○ RSPP e addetti SPP</li></ul>
Luoghi di custodia del materiale cartaceo	(Vedi scheda 7. Elenco luoghi)		
Luogo di custodia dei supporti di memorizzazione informatici	Server e PC (Vedi scheda 9 Elenco Strumenti)		
Banche Dati Utilizzate	Personale (Vedi scheda 8- Elenco banche dati)		
Tipologia di accesso al digitale	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)		
Tipologia di accesso al cartaceo	(Vedi scheda 7. Elenco luoghi)		
Tipologia di connessione	ADSL tramite rete locale LAN		

<b>Codice</b>	<b>Tr.2</b>			
<b>Nome del trattamento</b>	<b>Gestione del contenzioso e procedimenti disciplinari</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	Tutte le attività relative alla difesa in giudizio del MIUR e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato, Ved. Regolamento Min. Pubblica Istruzione )</b>	<ul style="list-style-type: none"><li>○ <b>Finalità di rilevante interesse pubblico perseguite</b></li><li>○ <b>Norme relative al personale amministrativo del MIUR</b></li><li>○ <b>Norme per il personale delle istituzioni scolastiche</b></li><li>○ <b>Norme per il personale AFAM</b></li><li>○ <b>Norme per il personale IRRE</b></li></ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>		<b>Elaborazione</b>	
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si
<b>Particolari forme di elaborazione</b>	<b>Comunicazione con altri soggetti pubblici o privati</b> <ul style="list-style-type: none"><li>• <b>Ministero del Lavoro e delle Politiche Sociali:</b> per lo svolgimento <b>dei tentativi obbligatori di conciliazione</b> dinanzi a Collegi di conciliazione ex D.Lgs.30 marzo 2001, n. 165 (Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche.);</li><li>• <b>Organi arbitrali:</b> per le svolgimento delle procedure arbitrali ai sensi dei CCNL di settore;</li><li>• <b>Avvocature dello Stato:</b> per la difesa erariale e consulenza presso gli organi di giustizia;</li><li>• <b>Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria:</b> per l'esercizio dell'azione di giustizia;</li><li>• <b>Liberi professionisti, ai fini di patrocinio o di consulenza,</b> compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.</li></ul>			



<b>Struttura che concorre al trattamento</b>	<ul style="list-style-type: none"><li>○ Dirigente Scolastico</li><li>○ Direttore amministrativo (DSG)</li><li>○ Segreteria Amministrativa e Assimilati</li></ul>		
<b>Luoghi di custodia del materiale cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Luogo di custodia dei supporti di memorizzazione informatici</b>	Server e PC (Vedi scheda 9 – Elenco Strumenti)		
<b>Banche Dati Utilizzate</b>	Personale (Vedi scheda 8- Elenco banche dati)		
<b>Tipologia di accesso al digitale</b>	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)		
<b>Tipologia di accesso al cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Tipologia di connessione</b>	ADSL tramite rete locale LAN		
<b>Natura dei dati trattati</b>	<b>Comuni</b>	<b>Sensibili</b>	<b>Giudiziari</b>
	Si	Si	NO



<b>Codice</b>	<b>Tr.3</b>			
<b>Nome del trattamento</b>	<b>Organismi collegiali e commissioni istituzionali</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	Per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del MIUR e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali. Il dato sensibile trattato è <u>quello dell'appartenenza alle organizzazioni sindacali</u> , con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentanti delle organizzazioni sindacali.			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato, Ved. Regolamento Min. Pubblica Istruzione )</b>	<ul style="list-style-type: none"><li>○ Finalità di rilevante interesse pubblico perseguite</li><li>○ Norme Comuni</li></ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>		<b>Elaborazione</b>	
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si
<b>Particolari forme di elaborazione</b>	<ul style="list-style-type: none"><li>• <u>Nessuna</u></li></ul>			
<b>Natura dei dati trattati</b>	<b>Comuni</b>		<b>Sensibili</b>	<b>Giudiziari</b>
	Si		Si	NO
<b>Struttura che concorre al trattamento</b>	<ul style="list-style-type: none"><li>○ Dirigente Scolastico</li><li>○ Direttore amministrativo (DSG)</li><li>○ Segreteria Amministrativa e Assimilati</li></ul>		<ul style="list-style-type: none"><li>○ Collaboratori del D.S.,</li><li>○ Docenti,</li><li>○ Collaboratori scolastici,</li><li>○ Membri esterni organi collegiali</li></ul>	
<b>Luoghi di custodia del materiale cartaceo</b>	(Vedi scheda 7. Elenco luoghi)			
<b>Luogo di custodia dei supporti di memorizzazione informatici</b>	Server e PC (Vedi scheda 9 Elenco Strumenti)			
<b>Banche Dati Utilizzate</b>	Personale (Vedi scheda 8- Elenco banche dati)			
<b>Tipologia di accesso al digitale</b>	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)			
<b>Tipologia di accesso al cartaceo</b>	(Vedi scheda 7. Elenco luoghi)			
<b>Tipologia di connessione</b>	ADSL tramite rete locale LAN			



<b>Codice</b>	<b>Tr.4</b>			
<b>Nome del trattamento</b>	<b>Attività propedeutiche all' avvio dell'anno scolastico</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	<p><i>I dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi <u>convitti, educandi e scuole speciali</u>.</i></p> <p>Nell'espletamento delle attività propedeutiche all'avvio dell'anno scolastico da parte delle istituzioni scolastiche, possono esseri trattati dati sensibili relativi:</p> <ul style="list-style-type: none"> <li>• alle <u>origini razziali ed etniche</u>, per favorire l'integrazione degli alunni con cittadinanza non italiana;</li> <li>• alle <u>convinzioni religiose</u>, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;</li> <li>• allo <u>stato di salute per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi</u>;</li> <li>• alle vicende <u>giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione</u>; i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un <u>programma di protezione nei confronti dell'alunno</u> nonché nei confronti degli <u>alunni che abbiano commesso reati</u>.</li> </ul>			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato, Ved. Regolamento Min. Pubblica Istruzione )</b>	<ul style="list-style-type: none"> <li>○ Finalità di rilevante interesse pubblico perseguite</li> <li>○ Norme Comuni</li> </ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>		<b>Elaborazione</b>	
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si
<b>Particolari forme di elaborazione</b>	<p><b><u>Comunicazione</u></b> <b><u>ai seguenti soggetti per le seguenti finalità:</u></b></p> <ul style="list-style-type: none"> <li>• <u>agli Enti Locali per la fornitura dei servizi ai sensi del D.Lgs. 32 marzo 1998, n. 112</u> , limitatamente ai dati indispensabili all'erogazione del servizio [Il D.Lgs tratta: Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59]</li> <li>• <u>ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica</u>, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;</li> <li>• <u>alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap</u> di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n.104 (Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate (GU 17.02.1992 N. 39 SO) Materia: handicap (anche di familiari), pubblico impiego e servizi pubblici, Assistenza, previdenza e assicurazioni).</li> </ul>			



Natura dei dati trattati	Comuni	Sensibili	Giudiziari
	Si	Si	Si
Struttura che concorre al trattamento	<ul style="list-style-type: none"> <li>○ Dirigente Scolastico</li> <li>○ Direttore amministrativo (DSG)</li> <li>○ Segreteria Amministrativa e Assimilati</li> </ul>	<ul style="list-style-type: none"> <li>○ Collaboratori del D.S.,</li> <li>○ Docenti,</li> <li>○ Collaboratori scolastici</li> </ul>	
Luoghi di custodia del materiale cartaceo	(Vedi scheda 7. Elenco luoghi)		
Luogo di custodia dei supporti di memorizzazione informatici	Server e PC (Vedi scheda 9 Elenco Strumenti))		
Banche Dati Utilizzate	Personale (Vedi scheda 8- Elenco banche dati)		
Tipologia di accesso al digitale	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)		
Tipologia di accesso al cartaceo	(Vedi scheda 7. Elenco luoghi)		
Tipologia di connessione	ADSL tramite rete locale LAN		

Lodice	Tr.5			
Nome del trattamento	Attività educativa, didattica e formativa, di valutazione			
Descrizione Sintetica del trattamento e del flusso informativo	<p>da parte delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali, <u>possono essere trattati dati sensibili relativi:</u></p> <ul style="list-style-type: none"> <li>• alle <u>origini razziali ed etniche per favorire l'integrazione</u> degli alunni con cittadinanza non italiana;</li> <li>• alle convinzioni religiose per garantire la libertà di credo religioso;</li> <li>• allo <u>stato di salute, per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;</u></li> <li>• ai dati <u>giudiziari</u>, per assicurare il diritto allo studio anche a <u>soggetti sottoposti a regime di detenzione;</u></li> <li>• alle <u>convinzioni politiche</u>, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori.</li> </ul> <p>I dati sensibili possono essere trattati per le attività di valutazione periodica e finale, per le <u>attività di orientamento e per la compilazione della certificazione delle competenze.</u></p>			
Descrizione delle Finalità perseguite ( <i>fonti normative sull'attività istituzionale cui il trattamento è collegato, Ved. Regolamento Min. Pubblica Istruzione</i> )	<ul style="list-style-type: none"> <li>○ Finalità di rilevante interesse pubblico perseguite</li> <li>○ Norme Comuni</li> </ul>			
Trattamento "ordinario" dei dati	<b>Raccolta</b>	<b>Elaborazione</b>		
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si



<p><b>Particolari forme di elaborazione</b></p>	<p><b>Comunicazione</b> <b>ai seguenti soggetti per le seguenti finalità:</b></p> <ul style="list-style-type: none"> <li>• <u>Alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni</u>, limitatamente ai dati indispensabili all'erogazione del servizio;</li> <li>• <u>agli Enti Locali per la fornitura dei servizi ai sensi del D.Lgs. 32 marzo 1998, n. 112</u>, limitatamente ai dati indispensabili all'erogazione del servizio (Il D.Lgs tratta: Conferimento di funzioni e compiti amministrativi dello Stato alle regioni ed agli enti locali, in attuazione del capo I della legge 15 marzo 1997, n. 59)</li> <li>• <u>ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica</u>, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio;</li> <li>• <u>agli Istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile;</u></li> <li>• <u>all'INAIL per la denuncia di infortuni ai sensi del D.P.R. n. 1124/1965 (testo unico delle disposizioni per l'assicurazione obbligatoria contro gli infortuni sul lavoro e le malattie professionali).</u></li> <li>• <u>alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione e la verifica del Piano Educativo Individuale, ai sensi della Legge 5 febbraio 1992, n.104 (Legge-quadro per l'assistenza, l'integrazione sociale e i diritti delle persone handicappate (GU 17.02.1992 N. 39 SO) Materia: handicap (anche di familiari), pubblico impiego e servizi pubblici, Assistenza, previdenza e assicurazioni).5</u></li> <li>• <u>ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro</u>, ai sensi della Legge 24 giugno 1997, n. 196 (1) e del D. Lgs. 21 aprile 2005, n. 77 (2) e, facoltativamente, <u>per attività di rilevante interesse sociale ed economico</u>, limitatamente ai dati indispensabili all'erogazione del servizio. (1) Tratta di: Norme in materia di promozione dell'occupazione. (2) Tratta di: Definizione delle norme generali relative all'alternanza scuola-lavoro, a norma dell'articolo 4 della legge 28 marzo 2003, n. 53. (GU n. 103 del 05/05/2005)</li> </ul>		
<p><b>Natura dei dati trattati</b></p>	<p><b>Comuni</b> Si</p>	<p><b>Sensibili</b> Si</p>	<p><b>Giudiziari</b> Si</p>
<p><b>Struttura che concorre al trattamento</b></p>	<ul style="list-style-type: none"> <li>○ Dirigente Scolastico</li> <li>○ Direttore amministrativo (DSG)</li> <li>○ Segreteria Amministrativa e Assimilati</li> </ul>	<ul style="list-style-type: none"> <li>○ Collaboratori del D.S.,</li> <li>○ Docenti</li> <li>○ Collaboratori scolastici</li> <li>○ Membri esterni organi collegiali</li> </ul>	
<p><b>Luoghi di custodia del materiale cartaceo</b></p>	<p>(Vedi scheda 7. Elenco luoghi)</p>		
<p><b>Luogo di custodia dei supporti di memorizzazione informatici</b></p>	<p>Server e PC (Vedi scheda 9 Elenco Strumenti)</p>		
<p><b>Banche Dati Utilizzate</b></p>	<p>Personale (Vedi scheda 8- Elenco banche dati)</p>		
<p><b>Tipologia di accesso al digitale</b></p>	<p>Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)</p>		
<p><b>Tipologia di accesso al cartaceo</b></p>	<p>(Vedi scheda 7. Elenco luoghi)</p>		
<p><b>Tipologia di connessione</b></p>	<p>ADSL tramite rete locale LAN</p>		



<b>Codice</b>	<b>Tr.7</b>			
<b>Nome del trattamento</b>	<b>Rapporti Scuola – Famiglie : gestione del contenzioso</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	tutte le attività connesse alla instaurazione di <u>contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni denunce all'autorità giudiziaria, etc.)</u> con gli alunni e con le famiglie,  e tutte le attività relative alla <u>difesa in giudizio delle istituzioni scolastiche</u> di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato, Ved. Regolamento Min. Pubblica Istruzione )</b>	<ul style="list-style-type: none"><li>○ Finalità di rilevante interesse pubblico perseguite</li><li>○ Norme Comuni</li></ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>		<b>Elaborazione</b>	
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si
<b>Particolari forme di elaborazione</b>	<b>Comunicazione</b> con altri soggetti pubblici e privati : <ul style="list-style-type: none"><li>• <b>Avvocature dello Stato</b>, per la difesa erariale e consulenza presso gli organi di giustizia;</li><li>• <b>Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria</b>, per l'esercizio dell'azione di giustizia;</li><li>• <b>Liberi professionisti</b>, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.</li></ul>			
<b>Natura dei dati trattati</b>	<b>Comuni</b>	<b>Sensibili</b>	<b>Giudiziari</b>	
	Si	Si	Si	
<b>Struttura che concorre al trattamento</b>	<ul style="list-style-type: none"><li>○ Dirigente Scolastico</li><li>○ Direttore amministrativo (DSG)</li><li>○ Segreteria Amministrativa e Assimilati</li></ul>		<ul style="list-style-type: none"><li>○ Collaboratori del D.S.</li><li>○ Docenti nelle commissioni</li><li>○ Membri di organi Collegiali</li><li>○ Collaboratori scolastici</li></ul>	
<b>Luoghi di custodia del materiale cartaceo</b>	(Vedi scheda 7. Elenco luoghi)			
<b>Luogo di custodia dei supporti di memorizzazione informatici</b>	Server e PC (Vedi scheda 9 Elenco Strumenti)			
<b>Banche Dati Utilizzate</b>	Personale (Vedi scheda 8- Elenco banche dati)			
<b>Tipologia di accesso al digitale</b>	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)			
<b>Tipologia di accesso al cartaceo</b>	(Vedi scheda 7. Elenco luoghi)			
<b>Tipologia di connessione</b>	ADSL tramite rete locale LAN			



<b>Codice</b>	<b>Tr.8</b>			
<b>Nome del trattamento</b>	<b>Gestione finanziaria e contabile</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, necessari alle attività di gestione finanziaria e contabile e all'amministrazione del bilancio			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato)</b>	<ul style="list-style-type: none"><li>○ Finalità di rilevante interesse pubblico perseguite</li><li>○ Norme Comuni</li></ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>	<b>Elaborazione</b>		
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si
<b>Particolari forme di elaborazione</b>	<b>Comunicazione di dati comuni a Enti Pubblici:</b> solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela (il Titolare dispone che sia necessaria una sua specifica autorizzazione). <b>Comunicazione di dati comuni a Privati:</b> solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela (il Titolare dispone che sia necessaria una sua specifica autorizzazione). <b>Comunicazione di dati sensibili o giudiziari: MAI</b>			

<b>Natura dei dati trattati</b>	<b>Comuni</b>	<b>Sensibili</b>	<b>Giudiziari</b>
	Si	Si	Si
<b>Struttura che concorre al trattamento</b>	<ul style="list-style-type: none"><li>○ Dirigente Scolastico</li><li>○ Direttore amministrativo (DSG)</li><li>○ Segreteria Amministrativa e Assimilati</li></ul>		<ul style="list-style-type: none"><li>○ Collaboratori del D.S.,</li><li>○ Collaboratori scolastici,</li><li>○ RSPP e addetti SPP</li></ul>
<b>Luoghi di custodia del materiale cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Luogo di custodia dei supporti di memorizzazione informatici</b>	Server e PC (Vedi scheda 9 Elenco Strumenti)		
<b>Banche Dati Utilizzate</b>	Personale (Vedi scheda 8- Elenco banche dati)		
<b>Tipologia di accesso al digitale</b>	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)		
<b>Tipologia di accesso al cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Tipologia di connessione</b>	ADSL tramite rete locale LAN		



<b>Codice</b>	<b>T.9</b>			
<b>Nome del trattamento</b>	<b>Fornitori e clienti</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, necessari alle attività di vendita, acquisto o fornitura di beni, servizi o consulenze			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato)</b>	<ul style="list-style-type: none"> <li>○ Finalità di rilevante interesse pubblico perseguite</li> <li>○ Norme Comuni</li> </ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>		<b>Elaborazione</b>	
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si
<b>Particolari forme di elaborazione</b>	<p><b>Comunicazione di dati comuni a Enti Pubblici:</b> solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).</p> <p><b>Comunicazione di dati comuni a Privati:</b> solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).</p> <p><b>Comunicazione di dati sensibili o giudiziari:</b> MAI</p> <p><b>Diffusione di dati comuni:</b> solo se previsti da specifica norma di legge</p> <p><b>Diffusione di dati particolari:</b> solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)</p> <p><b>Diffusione di dati di salute:</b> MAI</p> <p><b>Diffusione degli altri dati sensibili e dei dati giudiziari:</b> MAI</p>			

<b>Natura dei dati trattati</b>	<b>Comuni</b>	<b>Sensibili</b>	<b>Giudiziari</b>
	Si	Si	Si
<b>Struttura che concorre al trattamento</b>	<ul style="list-style-type: none"> <li>○ Dirigente Scolastico</li> <li>○ Direttore amministrativo (DSG)</li> <li>○ Segreteria Amministrativa e Assimilati</li> </ul>		<ul style="list-style-type: none"> <li>○ Collaboratori del D.S.</li> </ul>
<b>Luoghi di custodia del materiale cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Luogo di custodia dei supporti di memorizzazione informatici</b>	Server e PC (Vedi scheda 9 Elenco Strumenti)		
<b>Banche Dati Utilizzate</b>	Personale (Vedi scheda 8- Elenco banche dati)		
<b>Tipologia di accesso al digitale</b>	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)		
<b>Tipologia di accesso al cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Tipologia di connessione</b>	ADSL tramite rete locale LAN		



<b>Codice</b>	<b>Tc.10</b>			
<b>Nome del trattamento</b>	<b>Gestione Istituzionale</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	(Il trattamento concerne tutti i dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, non compresi nei precedenti trattamenti e necessari per la gestione dell'attività istituzionale)			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato)</b>	<ul style="list-style-type: none"> <li>○ Finalità di rilevante interesse pubblico perseguite</li> <li>○ Norme Comuni</li> </ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>		<b>Elaborazione</b>	
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si
<b>Particolari forme di elaborazione</b>	<p><b>Comunicazione di dati comuni a Enti Pubblici:</b> solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).</p> <p><b>Comunicazione di dati comuni a Privati:</b> solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).</p> <p><b>Comunicazione di dati sensibili o giudiziari:</b> MAI</p> <p><b>Diffusione di dati comuni:</b> solo se previsti da specifica norma di legge</p> <p><b>Diffusione di dati particolari:</b> solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)</p> <p><b>Diffusione di dati di salute:</b> MAI</p> <p><b>Diffusione degli altri dati sensibili e dei dati giudiziari:</b> MAI</p>			

<b>Natura dei dati trattati</b>	<b>Comuni</b>	<b>Sensibili</b>	<b>Giudiziari</b>
	Si	Si	Si
<b>Struttura che concorre al trattamento</b>	<ul style="list-style-type: none"> <li>○ Dirigente Scolastico</li> <li>○ Direttore amministrativo (DSG)</li> <li>○ Segreteria Amministrativa e Assimilati</li> </ul>		<ul style="list-style-type: none"> <li>○ Collaboratori del D.S.</li> </ul>
<b>Luoghi di custodia del materiale cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Luogo di custodia dei supporti di memorizzazione informatici</b>	Server e PC (Vedi scheda 9 Elenco Strumenti)		
<b>Banche Dati Utilizzate</b>	Personale (Vedi scheda 8- Elenco banche dati)		
<b>Tipologia di accesso al digitale</b>	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)		
<b>Tipologia di accesso al cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Tipologia di connessione</b>	ADSL tramite rete locale LAN		



<b>Codice</b>	<b>Tr.11</b>			
<b>Nome del trattamento</b>	<b>Gestione sito web dell'istituto</b>			
<b>Descrizione Sintetica del trattamento e del flusso informativo</b>	<p>Il trattamento concerne solo dati comuni, non sensibili e non giudiziari, relativi a soggetti giuridici o persone fisiche, per le quali apposita disposizione di legge prevede la possibilità di diffusione.</p> <p><input type="checkbox"/> Questo trattamento è attivato</p> <p><input type="checkbox"/> Questo trattamento non è attivato</p>			
<b>Descrizione delle Finalità perseguite (fonti normative sull'attività istituzionale cui il trattamento è collegato)</b>	<ul style="list-style-type: none"> <li>o Finalità di rilevante interesse pubblico perseguite</li> <li>o Norme Comuni</li> </ul>			
<b>Trattamento "ordinario" dei dati</b>	<b>Raccolta</b>	<b>Elaborazione</b>		
	Presso gli interessati	Presso terzi	In forma cartacea	Con modalità informatizzate
	Si	Si	Si	Si
<b>Particolari forme di elaborazione</b>	<p><b>Comunicazione di dati comuni a Enti Pubblici:</b> solo se autorizzati da specifica norma di legge o Regolamento (oppure decorsi 45 giorni dopo aver comunicato l'esigenza di questa comunicazione al Garante, se non ha espresso dissenso). Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).</p> <p><b>Comunicazione di dati comuni a Privati:</b> solo se autorizzati da specifica norma di legge o Regolamento. Per i dati particolari è necessaria particolare cautela(il Titolare dispone che sia necessaria una sua specifica autorizzazione).</p> <p><b>Comunicazione di dati sensibili o giudiziari:</b> MAI</p> <p><b>Diffusione di dati comuni:</b> solo se previsti da specifica norma di legge</p> <p><b>Diffusione di dati particolari:</b> solo se previsti da specifica norma di legge e con particolari cautele (il Titolare dispone che sia necessaria una sua specifica autorizzazione)</p> <p><b>Diffusione di dati di salute:</b> MAI</p> <p><b>Diffusione degli altri dati sensibili e dei dati giudiziari:</b> MAI</p>			

<b>Natura dei dati trattati</b>	<b>Comuni</b>	<b>Sensibili</b>	<b>Giudiziari</b>
	Si	Si	Si
<b>Struttura che concorre al trattamento</b>	<ul style="list-style-type: none"> <li>o Dirigente Scolastico</li> <li>o Direttore amministrativo (DSG)</li> <li>o Segreteria Amministrativa e Assimilati</li> </ul>		
<b>Luoghi di custodia del materiale cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Luogo di custodia dei supporti di memorizzazione informatici</b>	Server e PC (Vedi scheda 9 Elenco Strumenti)		
<b>Banche Dati Utilizzate</b>	Personale (Vedi scheda 8- Elenco banche dati)		
<b>Tipologia di accesso al digitale</b>	Server e PC (Vedi scheda 9 – Elenco Strumenti Informatici)		
<b>Tipologia di accesso al cartaceo</b>	(Vedi scheda 7. Elenco luoghi)		
<b>Tipologia di connessione</b>	ADSL tramite rete locale LAN		

**2. Distribuzione dei compiti e delle Responsabilità (regola 19.2)****2.1 Elenco dei responsabili al trattamento dei dati e relativi incaricati**

<b>Struttura:</b>	<b>Responsabile:</b>	<b>Trattamenti operati dalla struttura:</b>	<b>Compiti della struttura:</b>
Dirigente Scolastico Prof.ssa MARIA SAPONIERO	Dirigente Scolastico	Tutti	Direzione generale di tutte le attività, gestione delle pratiche riservate
<b>Incaricati Interni, Unità Organizzative Omogenee:</b>	<b>Responsabile:</b>	<b>Trattamenti operati dalla struttura:</b>	<b>Compiti della struttura:</b>
Collaboratori del DS	Dirigente Scolastico	Tutti (potenzialmente)	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Segreteria	D.G.S.A. se Responsabile del trattamento	Tutti Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Corpo Docente	Dirigente Scolastico	Tr.3, Tr.4, Tr.5, Tr.7, Tr.8, Tr.9, Tr.10 Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività (Biblioteca, scelte degli acquisti, commissioni varie, ecc.)
Collaboratori sc. e personale ausiliario	D.G.S.A. se Responsabile del trattamento	Tutti, ma con attività di supporto. Tr .3 anche dati sindacali. In casi eccezionali: Tr.1, Tr.5 (dati sensibili). Se membri di commissione Tr.2 (dati sensibili o giudiziari).	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni, docenti e familiari
Membri ESTERNI di Organi Collegiali	Dirigente Scolastico	Tr.3 e tutti gli altri (tranne Tr.6) limitatamente alle strette esigenze della funzione	Partecipazione alle attività gestionali e alle scelte organizzative e di orientamento generale, nonché il CDI e la GE decisioni di tipo amministrativo, finanziario, regolamentare
<b>Incaricati Interni Con Compiti Specifici O Ulteriori:</b>	<b>Responsabile:</b>	<b>Trattamenti Operati Dalla Struttura:</b>	<b>Compiti Della Struttura:</b>
Incaricato del Backup periodico e coordinatore del <Disaster recovery> e delle prove di ripristino: PARISI Massimo	Dirigente Scolastico o Responsabile dei trattamenti	Tutti, ma limitatamente alla funzione	Esegue il backup almeno settimanale degli archivi informatici contenenti dati personali. Coordina l'impostazione del piano di



	in questione		recupero in caso di disastro informatico che comporti l'inagibilità del sistema o la perdita di dati personali. Coordina le prove obbligatorie di efficienza del backup e di ripristino dei dati dalla copia di salvataggio.
Custode delle chiavi degli archivi ad accesso controllato. E vice-custode delle chiavi. ALLOCCA GIUSEPPE	Dirigente Scolastico o Responsabile dei trattamenti in questione	Tutti i trattamenti non informatici, ma limitatamente alla funzione	E' l'unico detentore delle chiavi degli archivi ad accesso controllato e consegna all'Incaricato autorizzato all'accesso a un certo archivio la relativa chiave; la riceve di ritorno non appena cessata l'attività. Il vice lo sostituisce in caso di assenza.
Custode delle passwords: ROSETTA MASSANOVA	Dirigente Scolastico o Responsabile dei trattamenti in questione	Tutti i trattamenti informatici, ma limitatamente alla funzione	Da ogni Incaricato munito di accesso al computer mediante password, ad ogni scadenza della password (3 o 6 mesi, a seconda dei casi) riceve una busta chiusa contenente la password, da tenere a disposizione in caso di necessità di accesso agli archivi elettronici di quell'Incaricato quando è assente
R.S.P.P. Prof. Zoccola Antonio  Addetti al S.P.P. Nominati	Dirigente Scolastico	I trattamenti relativi all'applicazione della normativa 626 o ad essa riferiti:  Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare:  Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.  Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari	Applicazione normativa Dlgs 626/1994 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale



		Tr.3 Organismi collegiali e commissioni istituzionali  Tr.4 Attività propedeutiche all' avvio dell'anno scolastico  Tr.5 Attività educativa, didattica e formativa, di valutazione	
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con Handicap	Dirigente Scolastico	tutti i trattamenti informatizzati e non relativi all'attività  Tr.4 Attività propedeutiche all' avvio dell'anno scolastico  Tr.5 Attività educativa, didattica e formativa, di valutazione	Gestione di alunni con handicap didattico grave
Personale incaricato della creazione e gestione del sito web : Prof. Iuliano Nicola	Dirigente Scolastico	I trattamenti informatici, rigorosamente nei limiti relativi alle seguenti funzioni: Tr. 11 Gestione sito web dell'istituto	Creazione e gestione del sito web dell'Istituto
<b>Responsabili Interni Di Trattamento:</b>	<b>Responsabile:</b>	<b>Trattamenti operati dalla struttura:</b>	<b>Compiti della struttura:</b>
RESPONSABILE DI TRATTAMENTI: Direttore Servizi Generali Amm.vi	Dirigente Scolastico	Tutti i trattamenti, limitatamente alla gestione amministrativo-contabile e alla gestione delle attività dei Collaboratori Scolastici.	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
<b>Incaricati esterni:</b>	<b>Responsabile:</b>	<b>Trattamenti operati dalla struttura:</b>	<b>Compiti della struttura:</b>



Medico competente ai sensi del Dlgs 626/1994	Dirigente Scolastico	<p>I trattamenti relativi all'applicazione della normativa 626 o ad essa riferiti:</p> <p>Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni, in particolare:</p> <p>Tr.1 Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente ecc.</p> <p>Tr.2 DIPENDENTI E ASSIMILATI :Gestione del contenzioso e procedimenti disciplinari</p> <p>Tr.3 Organismi collegiali e commissioni istituzionali</p> <p>Tr.4 Attività propedeutiche all' avvio dell'anno scolastico</p> <p>Tr.5 Attività educativa, didattica e formativa, di valutazione</p>	Applicazione normativa Dlgs 626/1994 e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale
<b>Responsabili Esterni:</b>	<b>Responsabile:</b>	<b>Trattamenti Operati Dalla Struttura:</b>	<b>Compiti Della Struttura:</b>
RESPONSABILE ESTERNO DEL TRATTAMENTO : organizzazione per la manutenzione del Software <b>ARGO SRL</b>	Dirigente Scolastico	Tutti i trattamenti informatici , ma rigorosamente nei limiti della funzione	Manutenzione del software



### 3. Analisi dei rischi che incombono sui dati (regola 19.3)

Si metteranno di seguito in evidenza i rischi propri, connessi al trattamento dei dati personali secondo le categorie di rischio elencate nell'articolo 31 del D.Lgs 196/03.

Tali rischi si possono classificare in:

- distruzione o perdita, anche accidentale dei dati;
- connessi alla integrità dei dati;
- accesso non autorizzato ai dati;
- trattamento non consentito o non conforme alla finalità della raccolta;
- connessi con l'utilizzo di reti di telecomunicazione disponibili al pubblico;
- connessi al reimpiego di supporto di memorizzazione;
- connessi alla conservazione della documentazione relativa al trattamento;
- connessi all'utilizzo di archivi e contenitori con serrature.

#### **Rischi riguardanti le basi di dati trattate da docenti.**

I rischi sottoelencati afferiscono al trattamento dei dati connesso con l'attività didattica, che viene effettuato senza l'ausilio di strumenti elettronici,

- distruzione o perdita accidentale dei dati a causa di eventi naturali,
- allagamenti, furto danneggiamento etc.;
- connessi alla integrità dei dati: utilizzo di supporti o modalità di trattamento non stabili;
- accesso non autorizzato ai dati, da parte di soggetti esterni alla scuola o da parte di personale interno;
- trattamento non consentito o non conforme alle finalità di raccolta : diffusione, comunicazione, manomissione;
- connessi all'utilizzo di archivi e contenitori con serrature.

#### **Rischi riguardanti le basi di dati trattate dal personale Amministrativo.**

Riguardano le basi di dati trattate esclusivamente dal personale ATA ed anche la documentazione didattica su cui operano i docenti non riferita all'anno scolastico in corso; il trattamento è effettuato con strumenti elettronici e con strumenti non elettronici.

I rischi di cui si tratta sono:

- distruzione o perdita accidentale dei dati a causa di eventi naturali,
- allagamenti, furto, danneggiamento etc.;
- connessi alla integrità dei dati: utilizzo di supporti o modalità di trattamento non stabili;
- accesso non autorizzato ai dati , da parte di soggetti esterni alla scuola o da parte di personale interno;
- trattamento non consentito o non conforme alle finalità di raccolta: diffusione, comunicazione, manomissione,
- connessi all'utilizzo di archivi e contenitori con serrature;
- connessi all'utilizzo del sistema informativo automatizzato.



### Analisi dei rischi per il sistema informativo automatizzato.

L'analisi dei rischi consiste nella individuazione degli elementi del sistema informativo automatizzato (SIA) che necessitano di protezione e delle minacce cui gli stessi possono essere sottoposti, tenendo conto del fattore tecnologico e del fattore umano.

#### Risorse hardware

##### Elementi da proteggere:

- terminali
- Server
- P.C.
- stampanti
- disk drive
- linee di comunicazione

##### Minacce cui sono sottoposti

- malfunzionamenti dovuti a guasti
- malfunzionamenti dovuti a sabotaggi
- malfunzionamenti dovuti ad eventi naturali
- malfunzionamenti dovuti a furti e intercettazioni

#### Risorse software

##### Elementi da proteggere:

- Sistemi Operativi
- Software di Base
- Software Applicativi
- Gestori di basi di dati
- Software di rete

##### Minacce

- errori involontari contenuti nelle procedure che possono consentire ad utenti non autorizzati
- l'esecuzione di operazioni riservate
- presenza di codice malizioso, inserito volontariamente nell'applicazione al fine di svolgere operazioni non autorizzate o per danneggiare il programma (virus, cavalli di troia, bombe logiche, backdoor);
- attacchi denial of service

Dati (Si tratta del contenuto degli archivi, delle basi di dati, dati di transito, copie storiche, file di log, etc.)



Minacce

- accesso non autorizzato
- modifiche deliberate o accidentali

**Risorse professionali** (Si tratta di: amministratori di sistema, i sistemisti, i programmatori, gli operatori, gli addetti alla manutenzione, i consulenti, etc.)

Minacce

- attacchi sociali engineering attraverso i quali estranei cercano di ottenere informazioni per attaccare il sistema;
- scarsa consapevolezza in materia di sicurezza o motivi di rivalsa nei confronti dell'amministrazione;

**Supporti di memorizzazione** (Sono i supporti su cui vengono tenute le copie dei software installati, dei file di log e dei back-up)

Minacce

- distruzione o alterazione ad opera di eventi naturali
- distruzione o alterazione ad opera di azioni accidentali o intenzionali
- deterioramento nel tempo
- inaffidabilità del mezzo fisico
- evoluzione tecnologica del mercato.

In seguito si riportano le schede relative all'analisi dei rischi alla situazione attuale (data di rilevazione 9 novembre 2004)

**3.1 *Analisi dei rischi relativi ai luoghi***

<b>Rischio/Evento</b>	<b>Impossibilità di controllare l'accesso ai locali</b>
<b>Valutazione/gravità</b>	Medio
<b>Descrizione/impatto</b>	Impossibilità di controllare l'accesso ai locali
<b>Riferimento alle Misure</b>	- Antifurto - Vigilanza Esterna
<b>Luoghi</b>	Presidenza Direzione Amministrativa Segreteria Magazzino Archivio Storico

<b>Rischio/Evento</b>	<b>Eventi Naturali</b>
-----------------------	------------------------



<b>Valutazione/gravità</b>	Medio
<b>Descrizione/impatto</b>	Eventi Naturali
<b>Riferimento alle Misure</b>	- Progettazione
<b>Luoghi</b>	Presidenza Direzione Amministrativa Segreteria Magazzino Archivio Storico

<b>Rischio/Evento</b>	<b>Possibili Intrusioni</b>
<b>Valutazione/gravità</b>	Medio
<b>Descrizione/impatto</b>	Possibili Intrusioni non autorizzate ad i locali
<b>Riferimento alle Misure</b>	- Allarme
<b>Luoghi</b>	Presidenza Direzione Amministrativa Segreteria Magazzino Archivio Storico

<b>Rischio/Evento</b>	<b>Furti</b>
<b>Valutazione/gravità</b>	Medio
<b>Descrizione/impatto</b>	Furti di materiale
<b>Riferimento alle Misure</b>	- Antifurto - Porte Blindate
<b>Luoghi</b>	Presidenza Direzione Amministrativa Segreteria Magazzino Archivio Storico

<b>Rischio/Evento</b>	<b>Accesso non Autorizzato</b>
<b>Valutazione/gravità</b>	Medio
<b>Descrizione/impatto</b>	Accesso di persone non autorizzate
<b>Riferimento alle Misure</b>	- Antifurto - Porte Blindate - Personale ATA
<b>Luoghi</b>	Presidenza Direzione Amministrativa Segreteria Magazzino Archivio Storico

### 3.2 Analisi dei rischi relativi ai software

<b>Rischio/Evento</b>	<b>Bugs</b>
<b>Valutazione/gravità</b>	Elevato
<b>Descrizione/impatto</b>	Bugs che minacciano l'integrità dei dati
<b>Riferimento alle Misure</b>	- Aggiornamento



Software	- Argo in Rete –Sissi – ARGO - Microsoft Office
----------	---

<b>Rischio/Evento</b>	<b>Modifiche</b>
Valutazione/gravità	Elevato
Descrizione/impatto	Modifiche al programma che possano cambiare i dati
Riferimento alle Misure	- Controllare le modifiche
Software	- Argo in Rete - ARGO - Microsoft Office

<b>Rischio/Evento</b>	<b>Aggressione da Virus</b>
Valutazione/gravità	Elevato
Descrizione/impatto	Virus Informatico trasmesso via posta elettronica, connessione ad internet e/o dischi infetti
Riferimento alle Misure	- Antivirus
Software	- Argo in Rete — ARGO - Microsoft Office

<b>Rischio/Evento</b>	<b>Spyware</b>
Valutazione/gravità	Elevato
Descrizione/impatto	Aggressione da Software in grado di trasmettere informazioni riservate
Riferimento alle Misure	- Antivirus - Sistema Antiintrusione digitale (Firewall)
Software	- Argo in Rete — ARGO - Microsoft Office

### 3.3 *Analisi dei rischi relativi agli strumenti hardware*

<b>Rischio/Evento</b>	<b>Uso non Autorizzato Hardware</b>
Valutazione/gravità	Medio
Descrizione/impatto	Uso non Autorizzato Hardware
Riferimento alle Misure	- Chiave - Password

<b>Rischio/Evento</b>	<b>Manomissione</b>
Valutazione/gravità	Basso
Descrizione/impatto	Manomissione
Riferimento alle Misure	- Password

<b>Rischio/Evento</b>	<b>Guasto</b>
Valutazione/gravità	Medio
Descrizione/impatto	Guasto
Riferimento alle Misure	- Manutenzione

<b>Rischio/Evento</b>	<b>Sabotaggio</b>
Valutazione/gravità	Basso
Descrizione/impatto	Sabotaggio
Riferimento alle Misure	- Password - Backup - Antifurto

<b>Rischio/Evento</b>	<b>Furto</b>
Valutazione/gravità	Medio
Descrizione/impatto	Furto



Riferimento alle Misure	- Antifurto
-------------------------	-------------

<b>Rischio/Evento</b>	<b>Intercettazione Trasmissione Dati</b>
Valutazione/gravità	Basso
Descrizione/impatto	Intercettazione Trasmissione Dati
Riferimento alle Misure	- Criptazione

<b>Rischio/Evento</b>	<b>Eventi Naturali</b>
Valutazione/gravità	Basso
Descrizione/impatto	Eventi Naturali
Riferimento alle Misure	- Backup

### 3.4 Analisi dei rischi relativi alle banche dati digitali

<b>Rischio/Evento</b>	<b>Accesso non Autorizzato</b>
Valutazione/gravità	Elevato
Descrizione/impatto	Accesso non Autorizzato
Riferimento alle Misure	- Sistema Antiintrusione digitale (Firewall) - Password - Sistema Antiintrusione digitale (Firewall) - Password

<b>Rischio/Evento</b>	<b>Cancellazione dati non autorizzata</b>
Valutazione/gravità	Molto Elevato
Descrizione/impatto	Cancellazione dati non autorizzata
Riferimento alle Misure	- Password

<b>Rischio/Evento</b>	<b>Perdita Dati</b>
Valutazione/gravità	Molto Elevato
Descrizione/impatto	Perdita Dati
Riferimento alle Misure	-Backup

<b>Rischio/Evento</b>	<b>Impossibilità ripristino copie di backup</b>
Valutazione/gravità	Basso
Descrizione/impatto	Impossibilità ripristino copie di backup
Riferimento alle Misure	- Manutenzione Backup

<b>Rischio/Evento</b>	<b>Sabotaggio Dati</b>
Valutazione/gravità	Basso
Descrizione/impatto	Sabotaggio Dati
Riferimento alle Misure	- Backup - Password - Backup - Password



#### 4. Misure in essere e da adottare (regola 19.4).

##### Definizione delle politiche di sicurezza per i trattamenti con strumenti elettronici

In considerazione del fatto che la quasi totalità dei dati trattati in ambito aziendale sono da annoverare fra i dati sensibili, tra l'altro, quasi sempre contestualmente presenti insieme ai dati comuni, la Scuola ha scelto di adottare le misure di sicurezza di cui al presente documento sia che si tratti di dati comuni, sia che si tratti di dati sensibili, che di dati giudiziari, calibrando le misure di sicurezza su quelle previste per i dati sensibili, ai sensi del D.L.vo 196/03, che offrono maggiori garanzie di sicurezza.

La sicurezza dei dati deve essere considerata da tutti gli utenti una componente delle attività quotidiane, e deve essere posta in essere con il fine di:

- impedire l'accesso indesiderato alla memoria fisica del personal computer o dell'unità hardware;
  - evitare l'uso improprio o manomissione del personal computer o del dispositivo hardware;
- In particolare gli utenti sono tenuti ad assicurare, nell'utilizzo quotidiano del dispositivo hardware:
- il mantenimento della loro integrità e riservatezza dei dati gestiti durante l'attività lavorativa;
  - la sicurezza nella trasmissione e nelle comunicazioni all'interno della Scuola e con l'esterno (Internet, altre Amministrazioni, etc.);
  - la sicurezza delle stazioni di lavoro e dei personal computer, prevenendo l'uso improprio delle apparecchiature da parte di terzi, e preservando, durante l'assenza, mediante le normali misure di sicurezza, il luogo di lavoro ove il dispositivo è collocato;
  - la tempestiva rilevazione e segnalazione di eventuali e/o presunti problemi di sicurezza.

Pertanto tutti gli utenti dovranno concorrere a proteggere le informazioni assegnate loro in gestione attraverso l'utilizzo “proprio” delle apparecchiature informatiche, in termini di:

- Accesso ai sistemi e ai dati;
- Uso delle credenziali, password di autenticazione informatica e dei profili di autorizzazione;
- Protezione delle informazioni attraverso la custodia delle chiavi di accesso (password) e relativi profili autorizzativi
- evitare la memorizzazione di password

Il presente documento deve intendersi come “misure minime per la sicurezza dei dati”.

I controlli tecnici e le verifiche della sicurezza dei sistemi informativi automatizzati dell'Azienda sono assegnati al Responsabile del Sistema Informativo (R.S.I.), che stabilisce le modalità per l'effettuazione dei controlli stessi.

Il R.S.I., provvede all'aggiornamento del presente documento, in accordo con le norme vigenti e con le indicazioni provenienti dal Responsabile della sicurezza dei dati e del titolare.

##### Analisi delle misure riguardanti la sicurezza fisica dei luoghi dove vengono effettuati i trattamenti tramite strumenti elettronici

<b>Misura</b>	<b>Porte con serratura</b>
<b>Descrizione</b>	Protezione dei locali contenente gli strumenti (PC e Server) atti al trattamento dei dati
<b>Rischio Contrastato</b>	Uso non Autorizzato Hardware, Sabotaggio, Furto
<b>Trattamenti</b>	Tutti
<b>Banche Dati</b>	Tutte
<b>Effettività</b>	In Essere



Data Scheda	31/03/2010
Data ultimo controllo	31/03/2010
Data prossimo controllo	Entro il 31/03/2012
Periodicità del controllo	Annuale
Tipologia della misura	Misura preventiva

Misura	<b>Antifurto</b>
Descrizione	Antifurto
Rischio Contrastato	Sabotaggio-Furto
Trattamenti	Tutti
Banche Dati	Tutte
Effettività	Da attivare
Data Scheda	31/03/2010
Data ultimo controllo	31/03/2010
Data prossimo controllo	Entro il 31/03/2012
Periodicità del controllo	Annuale
Tipologia della misura	Misura preventiva

### Sicurezza Fisica

#### Sicurezza delle apparecchiature hardware

Gli incaricati del trattamento provvedono alle misure di protezione tese a evitare accesso a persone non autorizzate ad archivi e banche dati contenenti dati personali e sensibili e protezione da eventi accidentali o involontari.

Tra le misure utilizzabili si citano:

- 1 protezione fisica, attraverso custodia in ambienti protetti, di apparecchiature di particolare rilievo quali: server, files server, dispositivi di immagazzinamento dati, hard-disk asportabili;
- 2 conservazione dei dati su supporti di vario tipo (dischi, nastri e altri), a lettura ottica, magnetica, elettronica e altri, in armadi muniti di valida serratura;
- 3 conservazione dei dati di backup e copia della documentazione di cifratura dati in appositi armadi muniti di valida serratura;
- 4 possibilità di inibire l'accesso ad unità di memoria asportabili attraverso dispositivi di bloccaggio muniti di serratura o, in mancanza, messa a punto di protocolli che prevedano l'asportazione dell'unità mobile a termine del periodo di lavoro e la relativa custodia secondo quanto precisato al punto 1.

In generale gli incaricati evitano comportamenti che possano mettere a rischio l'integrità o la riservatezza dei dati, per esigenze particolari, chiedono la consulenza dell' R.S.I.

#### Analisi delle misure riguardanti la sicurezza logica (Software, Dispositivi di rete, Organizzazione)

Misura	<b>Password Bios</b>
Descrizione	Aggiornamento periodico della password per evitare l'accesso
Rischio Contrastato	Uso non Autorizzato Hardware
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC



<b>Effettività</b>	In essere
<b>Data Scheda</b>	31/03/2010
<b>Data ultimo controllo</b>	31/03/2011
<b>Data prossimo controllo</b>	Entro il 30/09/2011
<b>Periodicità del controllo</b>	Semestrale
<b>Tipologia della misura</b>	Misura di correzione

<b>Misura</b>	<b>Password di rete</b>
<b>Descrizione</b>	Aggiornamento periodico delle password di rete
<b>Rischio Contrastato</b>	Manomissione- Sabotaggio - Accesso non Autorizzato - Cancellazione dati non autorizzata
<b>Trattamenti</b>	Tutti quelli trattati con Software
<b>Banche Dati</b>	Tutte quelle su Server/PC
<b>Effettività</b>	In essere
<b>Data Scheda</b>	31/03/2010
<b>Data ultimo controllo</b>	31/03/2011
<b>Data prossimo controllo</b>	Entro il 30/09/2011
<b>Periodicità del controllo</b>	Semestrale
<b>Tipologia della misura</b>	Misura Preventiva

<b>Misura</b>	<b>Manutenzione</b>
<b>Descrizione</b>	Manutenzione Periodica
<b>Rischio Contrastato</b>	Guasto
<b>Trattamenti</b>	Tutti quelli trattati con Software
<b>Banche Dati</b>	Tutte quelle su Server/PC
<b>Effettività</b>	In Essere
<b>Data Scheda</b>	31/03/2010
<b>Data ultimo controllo</b>	31/03/2010
<b>Data prossimo controllo</b>	Entro il 31/03/2012
<b>Periodicità del controllo</b>	Annuale
<b>Tipologia della misura</b>	Misura preventiva

<b>Misura</b>	<b>Backup</b>
<b>Descrizione</b>	Copie di Backup per il ripristino dei dati sabotati
<b>Rischio Contrastato</b>	Sabotaggio- Eventi Naturali - Perdita Dati
<b>Trattamenti</b>	Tutti quelli trattati con Software aRGO
<b>Banche Dati</b>	Tutte quelle su Server/PC
<b>Effettività</b>	In essere
<b>Data Scheda</b>	31/03/2010
<b>Data ultimo controllo</b>	31/03/2011
<b>Data prossimo controllo</b>	Entro il 30/09/2011
<b>Periodicità del controllo</b>	Semestrale
<b>Tipologia della misura</b>	Preventiva

<b>Misura</b>	<b>Criptazione</b>
<b>Descrizione</b>	Criptazione dei dati trasmessi
<b>Rischio Contrastato</b>	Intercettazione Trasmissione Dati
<b>Trattamenti</b>	Tutti quelli trattati con Software
<b>Banche Dati</b>	Tutte quelle su Server/PC
<b>Effettività</b>	31/03/2010



Data Scheda	31/03/2011
Data ultimo controllo	Entro il 30/09/2011
Data prossimo controllo	Semestrale
Periodicità del controllo	Annuale
Tipologia della misura	Preventiva

<b>Misura</b>	<b>Sistema Antiintrusione digitale (Firewall)</b>
Descrizione	Sistema Antiintrusione digitale Firewall software o hardware
Rischio Contrastato	Accesso non Autorizzato
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	Da attivare ENTRO IL 31/03/2011
Data Scheda	31/03/2010
Data ultimo controllo	31/03/2010
Data prossimo controllo	Entro il 31/03/2012
Periodicità del controllo	Annuale
Tipologia della misura	Preventiva

<b>Misura</b>	<b>Manutenzione Backup</b>
Descrizione	Manutenzione e Test Periodico del sistema di Backup
Rischio Contrastato	Impossibilità ripristino copie di backup
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	31/03/2010
Data ultimo controllo	31/03/2011
Data prossimo controllo	Entro il 30/09/2011
Periodicità del controllo	Semestrale
Tipologia della misura	Misura preventiva

<b>Misura</b>	<b>Aggiornamento Password</b>
Descrizione	Aggiornamento Periodico delle Password dei sistemi hardware e software correlati alla banca dati
Rischio Contrastato	Sabotaggio Dati
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	31/03/2010
Data ultimo controllo	31/03/2011
Data prossimo controllo	Entro il 30/09/2011
Periodicità del controllo	Semestrale
Tipologia della misura	Misura preventiva

<b>Misura</b>	<b>Aggiornamento Software</b>
Descrizione	Aggiornamento periodico del software
Rischio Contrastato	Bugs
Trattamenti	Tutti quelli trattati con Software
Banche Dati	Tutte quelle su Server/PC
Effettività	In essere
Data Scheda	31/03/2010



<b>Data ultimo controllo</b>	31/03/2011
<b>Data prossimo controllo</b>	Entro il 30/09/2011
<b>Periodicità del controllo</b>	Semestrale
<b>Tipologia della misura</b>	Misura preventiva

<b>Misura</b>	<b>Gestione Patch al Software</b>
<b>Descrizione</b>	Controllare le modifiche segnalate del software
<b>Rischio Contrastato</b>	Modifiche
<b>Trattamenti</b>	Tutti quelli trattati con Software
<b>Banche Dati</b>	Tutte quelle su Server/PC
<b>Effettività</b>	In essere
<b>Data Scheda</b>	31/03/2010
<b>Data ultimo controllo</b>	31/03/2011
<b>Data prossimo controllo</b>	Entro il 30/09/2011
<b>Periodicità del controllo</b>	Automatica o avviso
<b>Tipologia della misura</b>	Correttiva

<b>Misura</b>	<b>Antivirus</b>
<b>Descrizione</b>	Aggiornamento Periodico Antivirus
<b>Rischio Contrastato</b>	Aggressione da Virus-
<b>Trattamenti</b>	Tutti quelli trattati con Software
<b>Banche Dati</b>	Tutte quelle su Server/PC
<b>Effettività</b>	In essere
<b>Data Scheda</b>	31/03/2010
<b>Data ultimo controllo</b>	31/03/2011
<b>Data prossimo controllo</b>	Entro il 30/09/2011
<b>Periodicità del controllo</b>	Semestrale
<b>Tipologia della misura</b>	Preventiva

### Sicurezza Logica

#### *Controllo degli accessi ai sistemi di elaborazione*

L'accesso degli incaricati agli applicativi ed ai dati gestiti attraverso il Sistema Informativo avviene esclusivamente attraverso modalità prestabilite basate su quanto previsto dall'art. 34 del D.Lgs. n.196/03.

#### **In particolare:**

- 1 l'accesso ai sistemi è eseguito attraverso una procedura di identificazione dell'utente, denominata "autenticazione informatica", finalizzata alla verifica dell'identità o della dichiarazione dell'identità dell'utente;
- 2 l'"autenticazione informatica" avviene attraverso l'attribuzione di user-name e password (definito: account) agli operatori-utenti "custodi delle password" sulla base delle credenziali in possesso, ed il riconoscimento dell'utente da parte della procedura;
- 3 gli utenti accedono al sistema sulla base dell'identificazione e sono abilitati all'utilizzo delle procedure e all'accesso ai dati secondo il profilo di autorizzazione;
- 4 l'assegnazione del user-name e password (account) viene effettuata dal Sistema Informativo Aziendale su richiesta del "Responsabile del trattamento" che individua gli operatori-utenti



titolari dell'”autenticazione informatica” e indica il profilo autorizzativo per ogni “custode della password”.

***Tutti gli operatori-incaricati rispettano le seguenti disposizioni:***

- 5 L'utente cui viene assegnata una password di accesso al sistema e/o alla rete è responsabile di quanto accade a seguito di transazioni ed elaborazioni abilitate dalla propria password, e viene nominato “custode della password”;
- 6 la password è assegnata in maniera non riconducibile all'utente, né facilmente collegabile a nomi di parenti o date di nascita o similari; gli utenti devono essere ammoniti ed informati in tal senso, onde evitare la creazione di password banali e/o facilmente identificabili;
- 7 la password viene sostituita ogni tre mesi, indipendentemente se trattasi di password attribuita a profilo utente gestore di dati comuni o profilo utente gestore di dati sensibili;
- 8 le password sostituite non possono essere riciclate ed attribuite ad altro o nuovo utente;
- 9 in caso di inutilizzo della password per un periodo superiore ai tre mesi, la stessa viene dimessa e non attribuita ad alcun utente;
- 10 la password è disattivata anche in caso di perdita che consente all'incaricato l'accesso ai dati personali;
- 11 la lunghezza della password prevista dal sistema di autenticazione, è composta da 8 (otto) caratteri, e laddove la procedura non lo consenta, dal numero massimo di caratteri da questa previsto;
- 12 non è consentito l'accesso a sistemi diversi con lo stesso account (user-name e password) contemporaneamente; non è consentito utilizzare un medesimo account per accedere contemporaneamente alla stessa applicazione da diverse postazioni;
- 13 i documenti cartacei utilizzati per l'attribuzione dell'account, non devono essere conservati, o inseriti in ulteriori documenti (cartacei o informatici), in prossimità e comunque in evidenza del suo utilizzatore. I parametri di accesso al sistema vanno memorizzati, o in alternativa i supporti vanno conservati in luogo a parte e ad accesso esclusivo del suo titolare ed eventualmente le informazioni cifrate secondo un sistema di ri-codifica personale;
- 14 l'utente attiva tutte le misure in suo potere per evitare che terzi abbiano accesso al suo sistema mentre si allontana durante una sessione di lavoro: a tal fine esce dalla procedura e/o dal sistema (log-out), o lo blocca con una password, eventualmente tramite uno screen saver condizionato a password;
- 15 l'utente non comunica a nessuno le proprie password, neanche quelle vecchie non più in uso, per evitare il calcolo di regole empiriche utilizzate per la creazione delle stesse o eventuali ciclicità che non andranno, però, utilizzate nell'attribuzione di password;
- 16 Gli account di livello elevato (Administrator, root, super-utente) non vengono usati per il normale lavoro. Ogni utente cui sia stato assegnato un account di questo tipo dispone di almeno un altro account come utente normale;
- 17 Nel caso che l'utente disponga di più account, anche su macchine diverse, è opportuno che le password utilizzate siano diverse;
- 18 Gli utenti devono essere a conoscenza degli articoli del Codice Penale, 615 ter – “Accesso abusivo ad un sistema informatico o telematico” e 615 quater – “Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici”;
- 19 i Responsabili provvedono ad effettuare , almeno una volta all'anno, un aggiornamento dell'ambito del trattamento consentito ai singoli incaricati, addetti alla gestione e/o manutenzione degli strumenti elettronici;
- 20 i responsabili provvedono, altresì, ad effettuare almeno una volta all'anno la verifica della sussistenza delle condizioni per la conservazione o variazione dei profili di autorizzazione



### *Controllo del software e dell'hardware*

Appena viene scoperto un problema che può compromettere la sicurezza del sistema, l'utente ne dà comunicazione al R.S.I. Questi provvede ad analizzare il problema e adottare le misure tecniche necessarie a risolverlo (come installazione di patch, modifiche hardware o software, ecc.) anche attraverso persone specificamente delegate.

All'utente è vietato installare programmi non attinenti le normali attività d'ufficio, né nuove versioni di programmi già in uso né nuovi programmi necessari quali versioni client di applicativi gestionali, senza il preventivo parere del R.S.I.

Gli utenti non modificano le configurazioni hardware e software delle apparecchiature, senza il preventivo parere del R.S.I. .

### *Sicurezza Organizzativa*

Accanto all'adozione di misure tecnologiche già illustrate, è necessario, come richiamato, vengano definite una serie di norme e procedure miranti a regolamentare gli aspetti organizzativi del processo di sicurezza.

Gli aspetti organizzativi riguardano principalmente:

- la definizione di ruoli, compiti e responsabilità per la questione di tutte le fasi del processo Sicurezza;
- l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

Un ulteriore aspetto inerente la Sicurezza Organizzativa è quello concernente i controlli sulla consistenza e sulla affidabilità degli apparati.

In ordine alle norme di comportamento, si rimanda a quanto è definito nei documenti di nomina per l'assegnazione di responsabilità ed incarichi.



## 5. Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5)

Al fine di poter recuperare i dati a seguito di qualsiasi calamità si prevede di predisporre SEMPRE UNA COPIA DEI DATI con una almeno settimanale. La copia potrà essere eseguita con qualsiasi idoneo mezzo (nastri magnetici, CD, DVD, altri supporti per la memorizzazione di massa). Le copie dovranno essere segregate in altri locali rispetto a quelli in cui sono dislocati i supporti di memorizzazione, al fine di preservarli in caso di furto o incendio, dovranno essere custoditi a chiave ed affidati al Responsabile del Sistema Informativo (R.S.I.) nominato, secondo le disposizioni impartite nella lettera d’incarico.

La responsabilità sull’efficacia di tale sistema è assegnata al responsabile della gestione del sistema informatico.

Trimestralmente sarà necessario dare evidenza oggettiva di aver condotto un test di recupero dati dalla copia per verificare l’efficienza del sistema:

Per il ripristino dei dati il responsabile dei servizi informativi verifica ogni trimestre il funzionamento di questa attività. Procede alla copia di back-up dei dati dal supporto prescelto e attiva la procedura di ripristino verificando che il dato è effettivamente a disposizione.

Al fine di garantire che non si interrompa l’attività produttiva per un black-out causando perdite di dati o non reperibilità degli stessi è implementato per il server dove risiedono delle banche dati, un gruppo di continuità.

Trimestralmente sarà necessario dare evidenza oggettiva di aver condotto un test per verificare l’efficienza del sistema.

### Criteri e procedure per il salvataggio dei dati

Salvataggio			
Banca dati elettroniche	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio
Alunni Argo in Rete su Server	Un sistema periodico tramite software Sissi su server; uno automatico tramite procedura Windows di back up settimanale su unità nastro	Cassaforte in Segreteria con chiave custodita dalla Responsabile Del sistema Informativo	Responsabile del Sistema informativo
Personale Argo in Rete	Un sistema periodico tramite software Sissi su server; uno automatico tramite procedura Windows di back	Cassaforte in Segreteria con chiave custodita dalla Responsabile Del sistema Informativo	Responsabile del Sistema informativo



	up settimanale su Unità nastro		
Bilancio e contabilità Argo in Rete	Un sistema periodico tramite software Sissi su server; uno automatico tramite procedura Windows di back up settimanale su unità Nastro	Cassaforte in Segreteria con chiave custodita dalla Responsabile Del sistema Informativo	Responsabile del Sistema informativo

*Criteria e procedure per il ripristino della disponibilità dei dati*

<b>Ripristino</b>		
Banca dati elettroniche	Criteria e procedure per il ripristino dei dati	Pianificazione delle prove di ripristino
<i>Alunni</i> Argo in Rete	Si provvede a fare una copia di back up di dati e poi di verifica l'efficacia delle procedure di ripristino tramite software Restore di Windows, e verificarne la disponibilità dei dati	Sono previste prove di ripristino a cadenza mensile
<i>Personale</i> Argo in Rete	Si provvede a fare una copia di back up di dati e poi di verifica l'efficacia delle procedure di ripristino tramite software Restore di Windows, e verificarne la disponibilità dei dati	Sono previste prove di ripristino a cadenza mensile
<i>Bilancio e contabilità</i> Argo in Rete	Si provvede a fare una copia di back up di dati e poi di verifica l'efficacia delle procedure di ripristino tramite software Restore di Windows, e verificarne la disponibilità dei dati	Sono previste prove di ripristino a cadenza mensile



## 6. Formazione e pianificazione dei responsabili e degli incaricati al trattamento dei dati (regola 19.6)

Per renderli edotti i responsabili e gli incaricati 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 è **programmata la formazione già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali odì variazioni normative.**

Ciascun addetto dovrà prendere visione del DPS, studiarlo al fine di apprenderne il significato ed i contenuti. Nelle lettere di incarico si dovrà espressamente far riferimento a tutti i rischi ed alle relative misure previste per l'incaricato. Copia delle lettere d'incarico e della dichiarazione di presa visione e di apprendimento dei contenuti del DPS dovrà essere rilasciata da parte di ciascun incaricato.

Il responsabile del trattamento assume la responsabilità della formazione di ogni suo incaricato.

In particolare il corso dovrà garantire:

- Introduzione alle tematiche del decreto legislativo n. 196/03;
- Definizioni
- il Documento Programmatico sulla Sicurezza (DPSS).
- Trattamento dei dati e le misure minime di sicurezza;
- Le procedure di protezione: autenticazione informatica; la gestione delle credenziali e della riservatezza; il sistema di autorizzazione e protezione antivirus, l'aggiornamento dei software, il salvataggio dei dati
- Analisi dei rischi
- Interessato: 1- diritti ed esercizio; 2- modalità di esercizio e riscontro
- Il titolare dei dati: compiti e responsabilità
- Il responsabile della sicurezza: compiti e responsabilità
- Gli incaricati : compiti e responsabilità

Si è realizzata, il 30/03/2008 l'informazione di tutto il personale della scuola in servizio, docente e ATA, attraverso l'organizzazione di una specifica attività per complessive 8 ore.

Il personale supplente temporaneo che prenderà servizio durante il corso dell'anno scolastico verrà informato sui contenuti del codice e sui doveri da esso derivanti, anche attraverso la fornitura di materiale informativo di sintesi dal titolare o dal responsabile.



**7. Trattamenti affidati all'esterno (regola 19.7)**

***Non ci sono attività esternalizzate da parte di questo istituto.***



**8. Cifratura dei dati o separazione dei dati identificativi (regola 19.8)**

(Non riguarda la scuola, ma solo gli esercenti le professioni sanitarie).

**9. Elenco dei luoghi in cui si trattano i dati**

<b>LUOGO 1</b>	
Nome	Ufficio del Dirigente
Descrizione	Ufficio
Sede di appartenenza	Sede legale
Operatore	Dirigente Scolastico - Prof.ssa MARIA SAPONIERO
Responsabile	Dirigente Scolastico - Prof.ssa MARIA SAPONIERO
Modalità di accesso ai locali	Controllato dai collaboratori scolastici
Sistema di allarme	Non presente
Sistema di chiusura	Porta con serratura
Sistema antincendio	Piano di sicurezza della scuola.
Dotazioni e sistema di protezione	N°1 Archivio in metallo con chiave. N°. 1 PC desktop (PC 00)
<b>LUOGO 2</b>	
Nome	Ufficio Tecnico
Descrizione	Ufficio
Sede di appartenenza	Sede legale
Operatori	Parisi Massimo, Iennaco Giovanni
Responsabile trattamento dati	Rosetta Massanova
Modalità di accesso ai locali	Controllato dai collaboratori scolastici
Sistema di allarme	Centralizzato
Sistema di chiusura	Con serratura
Sistema antincendio	Presente
Dotazioni e sistema di protezione	N. 2 PC desktop ( 01, 02 ) N. 2 cassettiere in metallo N. 1 Armadio in legno N. 2 Armadi in metallo
<b>LUOGO 3</b>	
Nome	Ufficio contabilità
Descrizione	Ufficio
Sede di appartenenza	Sede legale
Responsabile	Rosetta Massanova
Operatori	Bosso Enrico
Modalità di accesso ai locali	Controllato dai collaboratori scolastici
Sistema di allarme	Centralizzato
Sistema di chiusura	Con serratura
Sistema antincendio	Presente
Dotazioni e sistema di protezione	N. 4 PC desktop ( 03, 04, 05, 05bis ) N. 2 armadi in metallo N. 3 cassettiere scrivanie
<b>LUOGO 4</b>	
Nome	Ufficio gestione assenze
Descrizione	Ufficio
Sede di appartenenza	Sede legale
Responsabile	Rosetta Massanova
Operatori	Perri Carmine, Marano Sofia
Modalità di accesso ai locali	Controllato dai collaboratori scolastici
Sistema di allarme	Centralizzato
Sistema di chiusura	Con serratura



<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N. 3 Pc Desktop ( 06, 07, 08 ) N. 6 cassettiere in metallo N. 3 Cassettiere scrivania N. 2 Armadi con ante in vetro
<b>LUOGO 5</b>	
<b>Nome</b>	Ufficio personale T.D.
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	<b>Morinelli Raffaele, Monaco Concettina</b>
<b>Responsabile</b>	<b>Rosetta Massanova,</b>
<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N.2 Armadi in metallo N. 3 Cassettiere scrivanie N. 3 Pc Desktop
<b>LUOGO 6</b>	
<b>Nome</b>	Ufficio didattica
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	<b>Coppola Anna Maria, Costagliola Maddalena, Santopaolo Alfonso</b>
<b>Responsabile</b>	<b>Rosetta Massanova</b>
<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N. 5 Pc _Desktop ( 12, 13, 14, 15, 16) N. 9 Cassettiere in metallo N. 3 Armadi in metallo
<b>LUOGO 7</b>	
<b>Nome</b>	Ufficio del DSGA
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	<b>Rosetta Massanova</b>
<b>Responsabile</b>	<b>Rosetta Massanova</b>
<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N. 1 Cassettiere in metallo N. 1 Armadio in metallo
<b>LUOGO 8</b>	
<b>Nome</b>	Intranet
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	<b>Parisi Massimo</b>
<b>Responsabile</b>	<b>Rosetta Massanova</b>



<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N. 8 cassettiere in metallo N°.3 PC di cui: 1 PC Server (PC 17) 2 Pc desktop (PC 18, 19)
<b>LUOGO 9</b>	
<b>Nome</b>	Ufficio protocollo
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	<b>Iuliano Concetta</b>
<b>Responsabile</b>	<b>Rosetta Massanova</b>
<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N. 2 Cassettiere in metallo N°2 PC desktop (20, 21)
<b>LUOGO 10</b>	
<b>Nome</b>	Magazzino
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	<b>Izzo Raffaella</b>
<b>Responsabile</b>	<b>Rosetta Massanova</b>
<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N. 2 Pc desktop ( 22, 23) N°.2 Archivi in metallo N°.1 Cassettera in metallo
<b>LUOGO 11</b>	
<b>Nome</b>	Centro Servizi
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	<b>Tutto il personale Amministrativo</b>
<b>Responsabile</b>	<b>DSGA</b>
<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N°.1 Archivio in metallo N°.1 Archivio in legno N°.3 Fotocopiatrici
<b>LUOGO 12</b>	
<b>Nome</b>	Ufficio personale T.D.
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	<b>Ruocco Pietro e Natella Carmela</b>



<b>Responsabile</b>	<b>DSGA</b>
<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N. 2 Pc desktop ( 24) N°.2 Cassettiere in metallo N°.1 accesso a sala fascicoli.
<b>LUOGO 13</b>	
<b>Nome</b>	Ufficio del Vicepreside
<b>Descrizione</b>	Ufficio
<b>Sede di appartenenza</b>	Sede legale
<b>Operatori</b>	Vicepreside
<b>Responsabile</b>	Vicepreside
<b>Modalità di accesso ai locali</b>	Controllato dai collaboratori scolastici
<b>Sistema di allarme</b>	Centralizzato
<b>Sistema di chiusura</b>	Con serratura
<b>Sistema antincendio</b>	Presente
<b>Dotazioni e sistema di protezione</b>	N. 1 Pc desktop ( 25) N°.1 Archivio in metallo

**10. Elenco delle banche dati utilizzate dai diversi trattamenti**

<b>Nome Banca Dati</b>	PERSONALE
<b>Descrizione della banca dati</b>	Anagrafica personale docente, non docente, di ruolo, non di ruolo, di sostegno, retribuzioni, certificazioni medico-sanitarie e contabilità fiscale.
<b>Formato Banca Dati</b>	Elettronico – cartaceo
<b>Tipo di dato trattato</b>	Dati Personali e sensibili e giudiziari
<b>Luogo in cui vengono trattati i dati</b>	Presidenza Direttore SGA Segreteria Archivio storico
<b>Trattamenti</b>	Vedi scheda 1 elenco dei trattamenti
<b>Modalità di diffusione dei dati</b>	Stampati in genere come da riferimenti normativi

<b>Nome Banca Dati</b>	ALUNNI – GENITORI
<b>Descrizione della banca dati</b>	Anagrafica alunni ed ex alunni, anagrafica genitori, pagelle, diplomi, certificazioni medico-sanitarie, valutazioni, documentazioni dello stato di Handicap, registri di classe e dei docenti.
<b>Formato Banca Dati</b>	Elettronico – cartaceo
<b>Tipo di dato trattato</b>	Dati Personali , sensibili e giudiziari
<b>Luogo in cui vengono trattati i dati</b>	Presidenza Direttore SGA Segreteria Archivio storico
<b>Trattamenti</b>	Vedi scheda 1 elenco dei trattamenti
<b>Modalità di diffusione dei dati</b>	Stampati in genere come da riferimenti normativi

<b>Nome Banca Dati</b>	BILANCIO – CONTABILITA’
<b>Descrizione della banca dati</b>	Bilancio di esercizio, buste paga, gestione fiscale, gestione patrimoniale, magazzino, gestione contratti e fornitori.
<b>Formato Banca Dati</b>	Elettronico – cartaceo
<b>Tipo di dato trattato</b>	Dati Personali e sensibili
<b>Luogo in cui vengono trattati i dati</b>	Presidenza Direttore SGA Segreteria Archivio storico
<b>Trattamenti</b>	Vedi scheda 1 elenco dei trattamenti
<b>Modalità di diffusione dei dati</b>	Stampati in genere come da riferimenti normativi

<b>Nome Banca Dati</b>	AFFARI GENERALI E PROTOCOLLO
<b>Descrizione della banca dati</b>	Posta in entrata e in uscita, protocollo in entrata e in uscita e corrispondenza generica.
<b>Formato Banca Dati</b>	Elettronico – cartaceo
<b>Tipo di dato trattato</b>	Dati Personali , sensibili e giudiziari
<b>Luogo in cui vengono trattati i dati</b>	Presidenza Direttore SGA



	Segreteria Archivio storico
<b>Trattamenti</b>	Vedi scheda 1 elenco dei trattamenti
<b>Modalità di diffusione dei dati</b>	Stampati in genere come da riferimenti normativi

<b>Nome Banca Dati</b>	ARCHIVIO STORICO CARTACEO
<b>Descrizione della banca dati</b>	Fascicoli riferiti alle banche dati non riferite al ciclo scolastico in corso.
<b>Formato Banca Dati</b>	Cartaceo
<b>Tipo di dato trattato</b>	Dati Personali , sensibili e giudiziari
<b>Luogo in cui vengono trattati i dati</b>	Locale archivio
<b>Trattamenti</b>	Vedi scheda 1 elenco dei trattamenti
<b>Modalità di diffusione dei dati</b>	Consultazione autorizzata e stampati in genere come ad riferimenti normativi
<b>Nome Banca Dati</b>	PROTOCOLLO RISERVATO DEL DIRIGENTE SCOLASTICO
<b>Descrizione della banca dati</b>	Protocollo in entrata e in uscita di documenti riservati personali.
<b>Formato Banca Dati</b>	Cartaceo
<b>Tipo di dato trattato</b>	Dati Personali , sensibili e giudiziari
<b>Luogo in cui vengono trattati i dati</b>	Presidenza
<b>Trattamenti</b>	Vedi scheda 1 elenco dei trattamenti
<b>Modalità di diffusione dei dati</b>	Nessuna

**11. Elenco degli strumenti con cui si trattano i dati**

<b>Strumento 0</b>			
Nome	PC_00		
Descrizione	Pc desktop		
Luogo di utilizzo	Luogo 1		
Descrizione luogo	Ufficio Presidenza		
Marca e modello	Pentium IV		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	Dirigente Scolastico		
Incaricato alla custodia delle password	DSGA		
Effettività Password	BIOS	Rete	SW
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows XP Professional		
Versione sistema operativo	XP Professional		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= Pentium 4		
Nome sw antivirus	Mc Afee virus scan		
Versione sw antivirus	2004		
Frequenza aggiornamento antivirus	Automatica		
Elenco dei software installati	Microsoft Office 2000 pro		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		

<b>Strumento 1</b>			
Nome	PC_01		
Descrizione	Pc desktop		
Luogo di utilizzo	luogo 2 UFFICIO TECNICO		
Descrizione luogo	Ufficio		
Marca e modello	P IV		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	PARISI Massimo		
Incaricato alla custodia delle password	DSGA		
Effettività Password	BIOS	Rete	SW
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows XP Professional -		
Versione sistema operativo	XP Professional		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= Pentium 4		
Nome sw antivirus	Mc Afee virus scan		
Versione sw antivirus	2004		
Frequenza aggiornamento antivirus	automatica		
Elenco dei software installati	Microsoft Office 2000 pro		
Accesso ad Internet	SI		



Tipo Di accesso	ADSL
Back up	Su server

Strumento 2			
Nome	PC_02		
Descrizione	Pc desktop		
Luogo di utilizzo	luogo 2 UFFICIO TECNICO		
Descrizione luogo	Ufficio		
Marca e modello	Pentium		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	Iannaco Giovanni		
Incaricato alla custodia delle password	DSGA		
Effettività Password	BIOS	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft XP Home Edition		
Versione sistema operativo	home edition		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= Pentium 4 2800+ RAM=512 HDD=80		
Nome sw antivirus	Antivir guard		
Versione sw antivirus	7.1		
Frequenza aggiornamento antivirus (scadenza)	Automatica		
Elenco dei software installati	Microsoft Office 2000 Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		

Strumento 3			
Nome	Pc 03		
Descrizione	Pc desktop UFFICIO CONTABILITA'		
Luogo di utilizzo	Scheda 8 Luogo 03		
Descrizione luogo	Ufficio		
Marca e modello	Pentium		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento			
Incaricato alla custodia delle password	DSGA		
Effettività Password	BIOS	Rete	Sw
	NO	SI	SI
Classificazione dello strumento	Pc desktop		
Soggetto a password	Si		
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Windows 2000 pro		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy,	CPU=Pentium 4		



cd-rom, dvd, dischi rigidi, ecc...)	
Nome sw antivirus	Mc Afee virus scan
Versione sw antivirus	
Frequenza aggiornamento antivirus (scadenza)	Automatica
Accesso ad Internet	SI
Tipo Di accesso	ADSL
Back up	Si
Elenco dei software installati	Argo

Strumento 4			
Nome	Pc_04		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 03 UFF. CONTABILITA'		
Descrizione luogo	Ufficio		
Marca e modello	Intel Celeron 1,1 Ghz		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	BOSSO ENRICO		
Incaricato alla custodia delle password	DSGA		
Effettività Password	Bios	Rete	Sw
	NO	SI	SI
Soggetto a password	Si		
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows xp professional		
Versione sistema operativo	4.0		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= Pentium 4		
Nome sw antivirus	Mcafee virus scan		
Versione sw antivirus	2004		
Frequenza aggiornamento antivirus (scadenza)	automatica		
Elenco dei software installati	Microsoft Office 2000 pro		
Accesso ad Internet	Si		
Tipo Di accesso	ADSL		
Back up	Su Server		

Strumento 5			
Nome	Pc_05		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 03		
Descrizione luogo	Ufficio		
Marca e modello	intel celeron 1,1 ghz		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento			
Incaricato alla custodia delle password	DSGA		
Effettività password	Bios	Rete	SW
	NO	NO	SI
Soggetto a password	Si		
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows xp professional		



Versione sistema operativo	4.0
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= celeron 1,1 ghz CPU_Speed=869 RAM=128 HDD=20 gb
Nome sw antivirus	Mcafee virus scan
Versione sw antivirus	2004
Frequenza aggiornamento antivirus (scadenza)	automatica
Elenco dei software installati	Microsoft Office 2000 pro
Accesso ad Internet	Si
Tipo Di accesso	ADSL
Back up	Su Server

<b>Strumento 05bis</b>			
Nome	Pc_05bis		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 03 ufficio contabilita'		
Descrizione luogo	Ufficio		
Marca e modello	intel celeron 1,1 ghz		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento			
Incaricato alla custodia delle password	DSGA		
Effettività password	Bios	Rete	SW
	NO	NO	SI
Soggetto a password	Si		
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows xp professional		
Versione sistema operativo	4.0		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= celeron		
Nome sw antivirus	Mcafee virus scan		
Versione sw antivirus	2004		
Frequenza aggiornamento antivirus (scadenza)	automatica		
Elenco dei software installati	Microsoft Office 2000 pro		
Accesso ad Internet	Si		
Tipo Di accesso	ADSL		
Back up	Su Server		

<b>Strumento 6</b>	
Nome	PC_06
Descrizione	Pc desktop
Luogo di utilizzo	Scheda 8 Luogo 4 gestione assenze
Descrizione luogo	Ufficio
Marca e modello	P IV
Manutentore	RSI
Incaricato all'utilizzo dello strumento	<b>Perri Carmine</b>
Incaricato alla custodia delle password	DSGA
Soggetto a password	Si



Effettività password	Bios	Rete	Sw
	NO	Si	Si
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows 2000 Professional -		
Versione sistema operativo	2000 Professional -		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU=intel p4		
Nome sw antivirus	MCAFEE		
Versione sw antivirus	AUTOMATICA		
Frequenza aggiornamento antivirus (scadenza)	GIORNALIERA		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		

**Strumento 7**

Nome	PC_04		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8		
Descrizione luogo	Ufficio		
Marca e modello	Pentium 3		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	Marano Sofia		
Incaricato alla custodia delle password	DSGA		
Soggetto a password	Si		
Effettività Password	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Sistema operativo	Microsoft Windows 2000 Professional –		
Versione sistema operativo	2000 pro		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU=P 4		
Nome sw antivirus	MCAFEE		
Versione sw antivirus	AUTOMATICA		
Frequenza aggiornamento antivirus (scadenza)	GIORNALIERA		
Elenco dei software installati	Microsoft Office 2000 pro – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		

**Strumento 8**

Nome	PC_08		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 4 UFFICIO PERSONALE		
Descrizione luogo	Ufficio		
Marca e modello	P IV		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento			
Incaricato alla custodia delle password	DSGA		



Soggetto a password	Si		
Effettività password	Bios	Rete	Sw
	NO	Si	Si
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows 2000 Professional -		
Versione sistema operativo	2000 Professional -		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU=intel p4		
Nome sw antivirus			
Versione sw antivirus			
Frequenza aggiornamento antivirus (scadenza)			
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		
<b>Strumento 9</b>			
Nome	Pc_09		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 05 Ufficio personale T.D.		
Descrizione luogo	Ufficio		
Marca e modello	intel celeron		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	Monaco Concettina		
Incaricato alla custodia delle password	DSGA		
Effettività password	Bios	RETE	SW
	NO	SI	SI
Soggetto a password	Si		
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows xp professional		
Versione sistema operativo	4.0		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= Pentium 4 CPU_Speed=2,8 ghz RAM=512 HDD=80 gb		
Nome sw antivirus	Mcafee virus scan		
Versione sw antivirus	2004		
Frequenza aggiornamento antivirus (scadenza)	automatica		
Elenco dei software installati	Microsoft Office 2000 pro		
Accesso ad Internet	Si		
Tipo Di accesso	ADSL		
Back up	Su Server		

<b>Strumento 10</b>			
Nome	PC_10		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 5 Ufficio personale T.D.		
Descrizione luogo	Ufficio		
Marca e modello	P IV		
Manutentore	RSI		



Incaricato all'utilizzo dello strumento	<b>Morinelli Raffaele</b>		
Incaricato alla custodia delle password	DSGA		
Soggetto a password	Si		
Effettività password	Bios	Rete	Sw
	NO	Si	Si
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows 2000 Professional -		
Versione sistema operativo	2000 Professional -		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= Pentium 4 CPU_Speed=2,8 ghz RAM=512 HDD=80 gb		
Nome sw antivirus	MCAFEE		
Versione sw antivirus	AUTOMATICA		
Frequenza aggiornamento antivirus (scadenza)	GIORNALIERA		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		

**Strumento 11**

Nome	PC_11		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 5 Ufficio personale T.D.		
Descrizione luogo	Ufficio		
Marca e modello	P IV		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento			
Incaricato alla custodia delle password	DSGA		
Soggetto a password	Si		
Effettività password	Bios	Rete	Sw
	NO	Si	Si
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows 2000 Professional -		
Versione sistema operativo	2000 Professional -		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU=intel p4 2.800 RAM=512 HDD=80 gb		
Nome sw antivirus	MCAFEE		
Versione sw antivirus	AUTOMATICA		
Frequenza aggiornamento antivirus (scadenza)	GIORNALIERA		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		

**Strumento 12**

Nome	PC_12		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 6 UFFICIO DIDATTICA		



Descrizione luogo	Ufficio		
Marca e modello	P IV		
Manutentore	RSI		
Incaricato alla custodia delle password	DSGA		
Soggetto a password	Si		
Effettività password	Bios	Rete	Sw
	NO	Si	Si
Possibilità di aggiornare autonomamente la password	Si		
Data scadenza password	30/09/2010		
Sistema operativo	Microsoft Windows xp Professional -		
Versione sistema operativo	xp Professional -		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU=intel p4 2.800 RAM=512 HDD=80 gb		
Nome sw antivirus	Mc Afee		
Versione sw antivirus	Virus scan		
Frequenza aggiornamento antivirus (scadenza)	GIORNALIERA		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		

<b>Strumento I3</b>			
Nome	PC_13		
Descrizione	Pc desktop		
Luogo di utilizzo	Scheda 8 Luogo 6 UFFICIO DIDATTICA		
Descrizione luogo	Ufficio		
Marca e modello	P IV		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	SANTOPAULO Alfonso		
Incaricato alla custodia delle password	DSGA		
Soggetto a password	Si		
Effettività password	Bios	Rete	Sw
	NO	Si	Si
Possibilità di aggiornare autonomamente la password	Si		
Sistema operativo	Microsoft Windows xp Professional -		
Versione sistema operativo	xp Professional -		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4		
Nome sw antivirus	MCAFEE		
Versione sw antivirus	AUTOMATICA		
Frequenza aggiornamento antivirus (scadenza)	GIORNALIERA		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		
<b>Strumento I4 -</b>			
Nome	PC-14		
Descrizione	Pc desktop		



Luogo di utilizzo	Ufficio 7 luogo 6		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	CASTAGLIOLA MADDALENA		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Sistema operativo	Microsoft Windows 2000 Professional -		
Versione sistema operativo	2000 pro		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4		
Data scadenza password	31/06/2007		
Sistema operativo	Microsoft Windows xp Professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		
<b>Strumento 15 -</b>			
Nome	PC-15		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 6		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento			
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Sistema operativo	Microsoft Windows 2000		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium		
Data scadenza password	30/09/2010		
Sistema operativo	Microsoft Windows xp Professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		
<b>Strumento 16 -</b>			
Nome	PC-16		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 6		
Descrizione luogo	Ufficio		



Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	COPPOLA ANNA MARIA		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Sistema operativo	Microsoft Windows 2000		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium		
Sistema operativo	Microsoft Windows xp Professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		
<b>Strumento 17 -</b>			
Nome	PC-17		
Descrizione	Pc desktop SERVER		
Luogo di utilizzo	Ufficio 7 luogo 8 INTRANET		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	PARISI Massimo		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Windows xp professional		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4		
Sistema operativo	Microsoft Windows xp Professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	SI		

<b>Strumento 18 -</b>			
Nome	PC-18		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 8		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		



Incaricato all'utilizzo dello strumento	PARISI Massimo		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Windows xp professional		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4		
Data scadenza password	30/09/2010		
Sistema operativo	Microsoft Windows xp Professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		

Strumento 19 -			
Nome	PC-19		
Descrizione	Pc server		
Luogo di utilizzo	Ufficio 7 luogo 8		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	PARISI Massimo		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Windows 2000 professional		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4 RAM=256 HDD=40 Unità backup 2,2 gb		
Sistema operativo	Microsoft Windows 2000 professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Sql aniware studio– Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	si		



Strumento 20 -			
Nome	PC-20		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 9- Ufficio Protocollo		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	IULIANO Concetta		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Windows 2000 professional		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4 RAM=256 HDD=40 Unità backup 2,2 gb		
Sistema operativo	Microsoft Windows 2000 professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Sql anyware studio– Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	si		



<b>Strumento 21 -</b>			
Nome	PC-21		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 9 - Ufficio Protocollo		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento			
Custode password	DSGA		
Soggetto a password	SI		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4		
Data scadenza password	30/06/2008		
Sistema operativo	Microsoft Windows xp Professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Microsoft Office 2000 – Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	Su server		



<b>Strumento 22</b>			
Nome	PC-22		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 10 MAGAZZINO		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento			
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Windows 2000 professional		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4 RAM=256 HDD=40 Unità backup 2,2 gb		
Sistema operativo	Microsoft Windows 2000 professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Sql aniware studio– Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	si		



<b>Strumento 23</b>			
Nome	PC-23		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 10 MAGAZZINO		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	IZZO RAFFAELLIA		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Windows 2000 professional		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4 RAM=256 HDD=40 Unità backup 2,2 gb		
Data scadenza password	30/09/2010		
Sistema operativo	Microsoft Windows 2000 professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Sql aniware studio– Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	si		



<b>Strumento 24</b>			
Nome	PC-24		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 12 Ufficio Personale T.D.		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	<b>Ruocco Pietro e Natella Carmela</b>		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Windows 2000 professional		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4		
Data scadenza password	30/09/2010		
Sistema operativo	Microsoft Windows 2000 professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Sql aniware studio– Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	si		



<b>Strumento 25</b>			
Nome	PC-25		
Descrizione	Pc desktop		
Luogo di utilizzo	Ufficio 7 luogo 13 VICEPRESIDE		
Descrizione luogo	Ufficio		
Marca e modello	P4		
Manutentore	RSI		
Incaricato all'utilizzo dello strumento	VICEPRESIDE		
Custode password	DSGA		
Soggetto a password	Si		
Effettività passwords	Bios	Rete	Sw
	NO	SI	SI
Possibilità di aggiornare autonomamente la password	SI		
Data scadenza password	Windows 2000 professional		
Sistema operativo	Xp		
Versione sistema operativo	2000		
Dotazione hardware dello strumento (se ha floppy, cd-rom, dvd, dischi rigidi, ecc...)	CPU= pentium 4 RAM=256 HDD=40 Unità backup 2,2 gb		
Sistema operativo	Microsoft Windows 2000 professional -		
Frequenza aggiornamento antivirus (scadenza)	Automatico		
Elenco dei software installati	Sql aniware studio– Argo		
Accesso ad Internet	SI		
Tipo Di accesso	ADSL		
Back up	si		



**Dichiarazioni finali e di impegno**

Obiettivo di questo Istituto è incrementare la sicurezza dei dati su supporto sia informatico che cartaceo e dei relativi archivi, pertanto si è proceduto ad un’attenta verifica delle condizioni di sicurezza degli archivi, in particolare quelli, separati o meno, contenenti dati sensibili/giudiziari. A seguito dell’analisi, saranno effettuati interventi incrementativi della sicurezza. Di questo c’è traccia negli allegati di questo documento.

Data \_\_\_\_\_ Firma del Titolare \_\_\_\_\_

Firma del Responsabile \_\_\_\_\_

Assunta al protocollo dell’Istituto: 31/03/2011 prot. 2739