*Ministero dell'Istruzione, dell'Università e della Ricerca*
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
**ISTITUTO COMPRENSIVO "ARISTIDE LEONORI"**
**INDIRIZZO MUSICALE**
Cod. Mecc. RMIC854008 - C.F. 80236250587 rmic854008@istruzione.it
*Via Achille Funi, 41 00125 – Roma 06/52311607 fax 065216211*
rmic854008@gigapec.it www.istitutoleonori.it

PROT. N. 1493/C1 ROMA, 10/03/2011
DECRETO N. 2570

# DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI (ANNO 2011)

(Artt. 33-36 del D.Lgs. 30/06/2003 n. 196. "*Codice in materia di protezione dei dati personali*".
A.S. 2010/2011

## IL DIRIGENTE SCOLASTICO

**VISTO** il **Decreto Legislativo 30 Giugno 2003, n. 196** ("*Codice in materia di protezione di dati personali")*, segnatamente l'art. 34 e ss. nonché *l'allegato B* del suddetto decreto, contenente il Disciplinare Tecnico in materia di misure minime di sicurezza;
**VISTO** il **Decreto Ministeriale 7 Dicembre 2006, n. 305** ("*Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, in attuazione degli artt. 20 e 21 del Decreto Legislativo 30 Giugno 2003, n. 196 recante Codice in materia di protezione dei dati personali")*;
**VISTO** il **Provvedimento del Garante per la Protezione dei Dati Personali, Delibera n. 13 del 01 Marzo 2007** *("Linee guida del Garante per posta elettronica ed Internet");*
**VISTO** il **Provvedimento del Garante per la Protezione dei Dati Personali, Delibera n. 23 del 14 Giugno 2007** *("Linee guida del Garante in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico");*
**VISTA** la **Direttiva del Ministero della Pubblica Istruzione n. 104 del 30 Novembre 2007** ("*Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche*");
**VISTO** il **Provvedimento generale del Garante per la Protezione dei Dati Personali del 27 Novembre 2008** *("Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema")* come modificato dai **Provvedimenti del 12 Febbraio e del 25 Giugno 2009;**

**CONSIDERATO** che l'Istituto Comprensivo "Aristide Leonori ", con sede a Roma in Via Achille Funi n. 41, in quanto dotato di un autonomo potere decisionale, ai sensi dell'art. 28 del *D.Lgs n. 196/ 2003*, deve ritenersi soggetto Titolare del trattamento di dati personali;
**ATTESO** che la Scuola, nell'espletamento delle funzioni istituzionali di formazione ed istruzione, raccoglie e tratta dati personali degli alunni e dei soggetti coinvolti a vario titolo nell'offerta formativa e, pertanto, è obbligata a prevedere ed applicare le "*misure minime di sicurezza"* di cui agli artt. 31 e ss. del *D.Lvo n. 196/2003*;
**RILEVATI** i cambiamenti avvenuti alla data odierna nella struttura organizzativa, amministrativa ed informatica dell'Istituto Scolastico, rilevanti agli effetti della disciplina del trattamento dei dati personali,

## DECRETA

E' adottato il presente "**Documento Programmatico sulla Sicurezza dei dati personali per l'anno 2011**", elaborato al fine di mettere in atto tutte le **"***misure di sicurezza"* finalizzate alla tutela dei dati personali oggetto di trattamento.
Si propone di delineare il quadro generale delle misure di protezione fisiche e logistiche da adottare per il trattamento dei dati effettuato dal personale della Scuola debitamente autorizzato, il cui rappresentante legale pro-tempore è il Dirigente Scolastico, nella persona della ***Dott.ssa Lina Porrello***, in qualità di **Titolare del trattamento dei dati personali.**
I provvedimenti organizzativi disposti e le misure di sicurezza adottate in osservanza di quanto disposto dal *D.Lgs 196/2003,* sono finalizzati a garantire a ciascun "interessato" (utente, dipendente, fornitore) la piena tutela dei diritti soggettivi quali appresso specificati:

- **diritto alla riservatezza** ed alla tutela della dignità personale, diritto all'identità personale;
- **diritto alla tutela dei dati personali**, allo scopo di evitare l'ingerenza di terzi;

- **diritto alla riservatezza delle documentazioni custodite dalla Scuola**, a salvaguardia nel tempo dell'integrità delle documentazioni medesime, siano esse costituite da materiale cartaceo che registrate su supporti informatici di memorizzazione.

## SCOPO DEL DOCUMENTO

Il presente Documento Programmatico sulla Sicurezza è adottato, ai sensi e per gli effetti previsti dagli Art. 33, 34, 35 e 36 del D.Lgs. n. 196/2003, per definire **le politiche di sicurezza in materia di trattamento di dati personali** ed i criteri organizzativi per la loro attuazione. Le disposizioni in esso contenute si applicano alle operazioni di trattamento dei dati compiute sia nella sede centrale dell'istituto di Via Funi 41, sia nel plesso aggregato di Via Funi 81.

## CAMPO DI APPLICAZIONE

Il Documento Programmatico sulla Sicurezza , in raccordo con la vigente normativa statale in materia di tutela delle persone rispetto al trattamento dei dati, individua le***" misure minime di sicurezza"*** in materia di trattamento dei dati personali effettuato presso l'istituzione scolastica nel normale svolgimento delle attività istituzionali.
Il documento disciplina le seguenti ***tipologie di dati personali***:

- **Dati Sensibili** (definiti dall'art. 22 della legge n. 675/96)
- **Dati Giudiziari** (individuati dall'art. 24 della legge n. 675/96)
- **Dati Comuni** (categoria residuale).

Il Documento si applica al trattamento di tutti i dati personali effettuato con le seguenti modalità:
a) mediante strumenti elettronici di elaborazione (trattamento informatico dei dati personali);
b) mediante l'utilizzo di altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

Eventuali situazioni di devianza rispetto a quanto precisato nel presente documento, accertate nel corso del monitoraggio delle procedure di gestione e trattamento dei dati personali che fanno capo all'istituto, dovranno essere rimosse nel più breve tempo possibile, sotto la vigilanza ed il coordinamento del Titolare del trattamento.

## DEFINIZIONI

Agli effetti del presente documento si richiamano le definizioni elencate nella Legge n. 675/1996, nel D.Lgs. n. 196/2003 e nel D.P.R. n. 318/1999, come di seguito riportate:

CATEGORIE GENERALI DI DATI:

***dati sensibili***, tassativamente individuati dall'art. 22 della legge n. 675/96: sono le informazioni che attengono alla sfera più intima del soggetto. Sono i dati idonei a rivelare "*l'origine razziale ed etnica*, *le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale";*

***dati giudiziari:*** individuati dall'art. 24 della legge n. 675/96, idonei a rivelare i provvedimenti di cui all'articolo 686, commi 1, lettere a) e d), 2 e 3, del codice di procedura penale (dati personali idonei a rivelare la sottoposizione di una persona a provvedimenti giudiziari che comportano l'iscrizione nel Casellario Giudiziario);

***dati comuni***, non espressamente definiti dal legislatore. Costituiscono una categoria residuale, ricavabile per esclusione rispetto alle elencazioni tassative di cui ai punti precedenti. Sono le informazioni riferite ad un soggetto, identificato o identificabile, non idonee a rivelare le informazioni elencate dagli articoli 22 e 24 della legge n. 675/96. A titolo meramente esemplificativo, si possono citare i dati anagrafici, fiscali, familiari, lavorativi, quelli attinenti alle abitudini di vita ed alle condizioni personali.

SPECIFICAZIONI TIPOLOGICHE:

| | |
|---|---|
| ***Amministratore di Sistema*** | soggetto cui è conferito il compito di sovrintendere alle risorse di una rete o di un sistema di basi di dati e di consentirne l'utilizzazione ad altri utenti; |
| ***autenticazione informatica*** | l'insieme degli strumenti elettronici e delle procedure per la verifica, anche indiretta, dell'identità di un operatore; |
| ***banca di dati*** | qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti; |

| | |
|---|---|
| ***blocco*** | la conservazione di dati personali con sospensione temporanea di ogni altra operazione di trattamento; |
| ***codice identificativo personale (user-id)*** | sequenza di codici numerici e alfanumerici in chiaro che identificano l'operatore che accede a un elaboratore, e che una volta assegnato ad una persona non deve poter essere più riutilizzato; |
| ***comunicazione elettronica*** | ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica; |
| ***credenziali di autenticazione*** | i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica; |
| ***custode delle password*** | persona incaricata di proteggere le buste sigillate contenenti le password di utenti ed incaricati, custodendole in apposita cassaforte o armadio blindato; |
| ***dati dei quali è consentita la comunicazione o diffusione*** | dati elencati dall'art. 20 L. 675/1996 (comunicazione consentita se vi è il consenso espresso dell'interessato, se i dati provengono da elenchi o registri pubblici o da documenti conoscibili da chiunque, in adempimento di un obbligo di legge); |
| ***dati giudiziari*** | i dati personali idonei a rivelare provvedimenti in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, ovvero la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale; |
| ***dati identificativi*** | i dati personali che permettono l'identificazione diretta e non equivoca dell'interessato; |
| ***dati personali comuni*** | qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili anche indirettamente mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale. In via residuale, sono tutti i dati personali non classificabili come sensibili o giudiziari; |
| ***dati personali sensibili*** | i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale; |
| ***diffusione*** | consiste nel dare conoscenza dei dati personali a soggetti indeterminati in qualunque forma, anche mediante la loro messa a disposizione, o consentendone la consultazione; |
| ***Documento Programmatico sulla Sicurezza*** | documento che definisce, sulla base dell'analisi dei rischi, le misure di sicurezza da adottare. Tale documento deve essere obbligatoriamente predisposto e revisionato con cadenza annuale, in presenza di dati personali trattati con elaboratori accessibili mediante una rete di telecomunicazione disponibile al pubblico; |
| ***Garante Privacy*** | l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675 con funzioni di controllo, vigilanza e consulenza; |

| | |
|---|---|
| ***Incaricati*** | le persone fisiche autorizzate, dal titolare o dal responsabile, a compiere operazioni di materiale trattamento dei dati personali; |
| ***interessato*** | la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali; |
| ***misure minime di sicurezza*** | il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31 del D.Lgs. n. 196/03; |
| ***parola chiave (password)*** | componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma crittografica; |
| ***posta elettronica*** | messaggi contenenti testi, voci, suoni o immagini trasmesse attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente; |
| ***profilo di autorizzazione*** | 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; |
| ***Responsabile*** | la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare alla gestione organizzata del sistema di trattamento di dati personali; |
| ***rete pubblica di comunicazioni*** | una rete di comunicazioni elettroniche utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico; |
| ***reti di comunicazione elettronica*** | i sistemi di trasmissione, le apparecchiature di commutazione o di instradamento e le altre risorse che consentono di trasmettere dati di vario genere o altri segnali; |
| ***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; |
| ***strumenti elettronici*** | gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento; |
| ***Titolare*** | la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza; |
| ***trattamento*** | qualunque operazione o complesso di operazioni, effettuate anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati; |
| ***utente*** | qualsiasi persona fisica che utilizza un servizio di |

comunicazione elettronica accessibile al pubblico.

**FONTI NORMATIVE DI RIFERIMENTO**

| | | | |
|---|---|---|---|
| - R.D. n. 633/1941 | - D. Lgs. n. 255/1997 | - D.Lgs. n. 51/1999 | - D.Lgs. n. 282/1999 |
| - D.Lgs. n. 518/1992 | - D.Lgs. n. 135/1998 | - D.Lgs. n. 135/1999 | - L. n. 325/2000 |
| - L. n. 675/1996 | - D.Lgs. n. 171/1998 | - D.P.R. n. 318/1999 | - D.Lgs. n. 196/2003 |
| - D.Lgs. n. 123/1997 | - D.Lgs. n. 389/1998 | - D.Lgs. n. 281/1999 | - L. n. 51/2006 |
| | | | - D.M. n. 305/2006. |

**ARTICOLAZIONE DEL DOCUMENTO**

Conformemente a quanto previsto dal punto 19 del "*Disciplinare tecnico allegato*" sub B) al *D.Lgs n. 196/2003*, nel presente documento sono evidenziati:

1. L'elenco dei trattamenti di dati personali.
2. L'indicazione delle sedi, la descrizione dei locali e degli strumenti con i quali si effettuano i trattamenti di dati personali.
3. La distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati.
4. L'analisi dei rischi che incombono sui dati.
5. Le misure minime di sicurezza adottate e da adottare per garantire l'integrità, la protezione, la salvaguardia ed il ripristino dei dati in seguito a distruzione o danneggiamento degli stessi.
6. La previsione e la pianificazione degli interventi formativi del personale interessato al trattamento dei dati e la definizione dei criteri e delle modalità di aggiornamento professionale del personale stesso.
7. La disciplina dei trattamenti di dati personali eventualmente affidati a soggetti esterni.
8. Le dichiarazioni di impegno programmatico.
9. L'obbligo di aggiornamento del DPS e le sue revisioni.

## 1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

**A. FINALITA':** per il perseguimento delle **finalità istituzionali**, che sono quelle relative **all'istruzione ed alla formazione degli alunni**, la Scuola tratta dati personali (comuni, sensibili o giudiziari) di studenti, personale dipendente, fornitori ed enti. I trattamenti sono effettuati, anche mediante l'utilizzo di strumenti elettronici, per le seguenti finalità:

- adempimento di **obblighi di fonte legislativa**, nazionale o comunitaria, regolamentare o derivante da atti amministrativi a contenuto particolare;
- erogazione dei servizi didattici e formativi;
- gestione dello stato giuridico del personale dipendente, docente ed ATA;
- adempimenti bancari, assicurativi, previdenziali ed assistenziali;
- tenuta della contabilità scolastica;
- gestione delle attività informative svolte ai sensi della Legge 7 giugno 2000 n. 150, recante la *"Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni";*
- attività strumentali e complementari alle finalità istituzionali.

**B. FONTE DEI DATI:** i dati trattati sono conservati su **supporti cartacei e/o informatici** e sono noti all'istituzione scolastica, in ragione della produzione:

- di atti o dichiarazioni provenienti da soggetti interessati a fruire dei servizi formativi, direttamente o a beneficio dei minori sottoposti alla potestà genitoriale;
- di documenti contabili connessi alla fornitura di beni e prestazioni di servizi o lavori;
- di documentazione bancaria, finanziaria e/o assicurativa;
- di documenti inerenti al rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/o previdenziali.

### 1.1 INFORMAZIONI DI BASE IN ORDINE AI TRATTAMENTI OPERATI

A) DOCUMENTI CONTENENTI DATI PERSONALI TRATTATI DAI DOCENTI

- Registro personale
- Elaborati degli alunni
- Registro di classe

- Registro dei verbali del consiglio di classe o di interclasse
- Documentazione relativa alla programmazione didattica
- Documenti di valutazione
- Schede personali degli alunni
- Documentazione dello stato di handicap
- Corrispondenza con le famiglie
- Documentazione giustificativa delle assenze degli alunni.

B) DOCUMENTI CONTENENTI DATI PERSONALI TRATTATI DAL PERSONALE AMMINISTRATIVO

- Fascicoli personali dei dipendenti in servizio presso la Scuola,
- Fascicoli degli alunni
- Albo dei fornitori
- Contratti, convenzioni e protocolli d'intesa
- Documentazione finanziaria e contabile
- Registro diplomi
- Registro infortuni degli alunni
- Certificazioni amministrative
- Certificazione sanitaria e medico-legale.

C) DOCUMENTI CONTENENTI DATI PERSONALI TRATTATI DAL DIRIGENTE SCOLASTICO

- Fascicoli del personale direttivo, docente ed ATA
- Verbali delle sedute degli Organi Collegiali
- Protocollo riservato
- Fascicoli del personale docente in prova
- Documentazione riservata e/o classificata di vario genere
- Corrispondenza riservata.

## 1.2 CLASSIFICAZIONE TIPOLOGICA DEI DATI PERSONALI TRATTATI

□ dati personali relativi agli alunni, quali nominativo, data di nascita, residenza, domicilio, stato di famiglia, codice fiscale, altri eventuali dati anagrafici; registri di classe contenenti i recapiti delle famiglie e comunicazioni varie;

□ "*dati sensibili"* relativi agli alunni (certificazioni mediche, certificazioni di handicap e disabilità, certificazione di idoneità alla pratica sportiva, diagnosi mediche) ; documentazione relativa alla scelta di avvalersi o meno dell'insegnamento della religione cattolica;

□ dati personali dei genitori degli alunni (istanze contenenti dati relativi alla situazione reddituale, economica e patrimoniale, documentazioni giudiziarie, documentazioni mediche prodotte a corredo delle domande di iscrizione o di altre istanze);

□ "*dati sensibili"* relativi ai dipendenti in servizio presso l'istituto;

□ dati personali riservati relativi ad alunni, genitori e personale dipendente riguardanti corrispondenza riservata custodita dal dirigente, compresi gli atti relativi ai provvedimenti disciplinari, protocollo riservato;

- □ dati personali relativi ai fornitori, riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la sede, la partita IVA, il codice fiscale;

- □ dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

- □ dati giudiziari riferibili a procedimenti pendenti in qualsiasi grado, di natura civile, penale, amministrativa, presso autorità giurisdizionali italiane ed estere.

### 1.3 NUOVA DISCIPLINA DEI DATI SENSIBILI E GIUDIZIARI

Il Ministero della Pubblica Istruzione, con **D.M. 7 Dicembre 2006 n. 305**, ha emanato il "***Regolamento per la disciplina del trattamento dei dati sensibili e giudiziari nel settore dell'Istruzione".***
Il suddetto Regolamento è stato recepito e formalmente adottato dal Consiglio d'Istituto con delibera n. 1 del 27 Febbraio 2007.

**A. OGGETTO DEL REGOLAMENTO** (ART. 1): il Regolamento reca, nelle **N. 7 Schede allegate** che ne formano parte integrante, la disciplina del trattamento dei dati sensibili e giudiziari effettuato nell'ambito delle funzioni istituzionali del Ministero della Pubblica Istruzione ed all'interno dell'istituzione scolastica , specificando in dettaglio:

- le **tipologie di dati** che possono essere trattati;
- l'**elenco dei trattamenti** consentiti;
- le **operazioni** che su di essi sono eseguibili;
- le **fonti normative** di riferimento;
- le **finalità di rilevante interesse pubblico** perseguite dalla Scuola;
- i **soggetti esterni**, pubblici e privati, a cui è possibile comunicare i dati.

Le Schede sopra citate disciplinano il trattamento dei dati sensibili e giudiziari relativamente alle seguenti materie:

- **Scheda n. 1 - Selezione e reclutamento a T.I. ed a T.D. e gestione del rapporto di lavoro;**
- **Scheda n. 2 - Gestione del contenzioso e procedimenti disciplinari;**
- **Scheda n. 3 - Organismi collegiali e commissioni istituzionali;**
- **Scheda n. 4 - Attività propedeutiche all'avvio dell'anno scolastico;**
- **Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione;**
- **Scheda n. 6 - Scuole non statali;**
- **Scheda n. 7 - Rapporti Scuola–Famiglia: gestione del contenzioso.**

Le Schede, che costituiscono una "guida obbligatoria "da cui la Scuola non può derogare, sono state portate a conoscenza diretta degli Incaricati del trattamento dei dati da parte del *Responsabile del trattamento dei dati*.

**B. INDIVIDUAZIONE DEI TIPI DI DATI E DI OPERAZIONI ESEGUIBILI** (ART. 2): i dati sensibili e giudiziari individuati dal Regolamento sono trattati previa verifica della loro **pertinenza, completezza e indispensabilità** rispetto alle finalità perseguite nei singoli casi, specie quando la raccolta non avvenga presso l'interessato.

- OPERAZIONI DI INTERCONNESSIONE, RAFFRONTO CON ALTRE BANCHE DATI E COMUNICAZIONE A TERZI
  Queste operazioni di trattamento dei dati sono ammesse soltanto se strettamente **indispensabili** allo svolgimento degli obblighi di volta in volta indicati e solo per il perseguimento di rilevanti **finalità di interesse pubblico** specificate. In ogni caso, le operazioni sopra indicate sono svolte previa indicazione scritta dei **motivi che ne giustificano l'effettuazione**, nel rispetto delle disposizioni in materia di protezione dei dati personali e degli altri limiti stabiliti dalla legge e dai regolamenti.

- INUTILIZZABILITA' DEI DATI
  Sono assolutamente **inutilizzabili** i dati trattati in violazione delle norme di legge e di regolamento in materia di trattamento dei dati personali.
  Il Titolare del trattamento vigila affinché il trattamento dei dati sensibili e giudiziari avvenga secondo modalità idonee a **prevenire violazioni dei diritti, delle libertà fondamentali e della dignità degli interessati**.

PROVVEDIMENTI DEL
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

**1. Deliberazione n. 13 del 1° Marzo 2007 ("*LINEE GUIDA PER POSTA ELETTRONICA ED INTERNET*"):**

è un provvedimento generale mediante il quale il Garante Privacy fornisce concrete indicazioni in ordine al corretto uso del computer sul luogo di lavoro, con particolare riferimento all'utilizzo della posta elettronica e della rete Internet;
la finalità del provvedimento è quella di **prevenire usi arbitrari ed impropri degli strumenti informatici** e tutelare, al contempo, il diritto alla riservatezza dei lavoratori.
L'Autorità prescrive ai datori di lavoro di informare con chiarezza e in modo dettagliato i lavoratori sulle **regole che disciplinano la navigazione su Internet e l'utilizzo della posta elettronica**, anche mediante l'adozione di un apposito "disciplinare " interno, da definire coinvolgendo anche le rappresentanze sindacali presenti sul luogo di lavoro.
Il Garante vieta poi la lettura e la registrazione sistematica delle e-mail così come il monitoraggio sistematico delle pagine web visualizzate dal lavoratore, perché ciò realizzerebbe un controllo a distanza dell'attività lavorativa vietato dallo Statuto dei lavoratori.

**2. Deliberazione n. 23 del 14 Giugno 2007** ("***LINEE GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI DI LAVORATORI PER FINALITÀ DI GESTIONE DEL RAPPORTO DI LAVORO IN AMBITO PUBBLICO***"):
lo scopo di questo provvedimento del Garante è quello di fornire indicazioni e raccomandazioni riguardo alle operazioni di trattamento effettuate con dati personali, anche sensibili, di lavoratori che svolgono servizio alle dipendenze di datori di lavoro pubblici.
Il datore di lavoro pubblico, nella fattispecie l'Istituzione Scolastica, può lecitamente trattare dati personali dei lavoratori **nella misura in cui ciò sia necessario per la corretta gestione del rapporto di lavoro**, avendo cura di applicare le disposizioni normative che disciplinano l'esercizio delle proprie funzioni istituzionali o il rapporto di lavoro, contenute in leggi, regolamenti, contratti e accordi collettivi di comparto.
Entrambi i provvedimenti del Garante hanno formato oggetto di diffusione al personale scolastico da parte del Titolare del trattamento dei dati (Dirigente Scolastico), per opportuna conoscenza e norma.
I punti più importanti del provvedimento sono i seguenti:

- **Dati sensibili e rapporto di lavoro:**
  l'amministrazione scolastica deve adottare maggiori cautele se le informazioni personali sono idonee a rivelare profili particolarmente delicati della vita privata dei propri dipendenti, quali la salute, le abitudini sessuali, le convinzioni politiche, sindacali, religiose, filosofiche o di altro genere, l'origine razziale ed etnica.
- **Assenze per malattia, certificati e visite mediche:**
  in caso di assenza per malattia, all'amministrazione vanno consegnati certificati medici privi di diagnosi e con la sola indicazione dell'inizio e della durata dell'infermità. Se il lavoratore produce documentazione in cui è presente anche la diagnosi, l'ufficio deve astenersi dall'utilizzare queste informazioni e deve invitare il personale a non produrre altri certificati con le stesse caratteristiche. Particolari cautele devono essere adottate dall'ente pubblico quando tratta dati relativi alla salute dei dipendenti nei casi di visite medico legali e denunce di infortunio all'Inail.
- **Diffusione dei dati personali su Internet:**
  l'amministrazione scolastica deve assicurare l'esattezza, l'aggiornamento e la pertinenza dei dati pubblicati in rete e garantire il "diritto all'oblio", cioè una tutela dinamica della riservatezza delle persone (trascorso un certo periodo dalla pubblicazione è opportuno spostare i nominativi in un parte del sito dove non siano più rintracciabili dai motori di ricerca esterni). Nelle graduatorie relative a concorsi o selezioni vanno riportati solo dati pertinenti (negli elenchi nominativi abbinati ai risultati o negli elenchi di ammessi alle prove scritte o orali, vige il divieto di pubblicare recapiti telefonici, codice fiscale ecc.) È sempre vietata la diffusione di informazioni sulla salute del lavoratore o dei familiari interessati.
- **Dati biometrici dei lavoratori pubblici:**
  anche nell'ambito del pubblico impiego non è consentito un uso generalizzato dei dati biometrici dei dipendenti (impronte digitali, iride, ecc.) per controllare le presenze o gli accessi sul luogo di lavoro. Il Garante può autorizzare l'attivazione di tali sistemi di rilevazione solo in presenza di particolari esigenze (aree adibite alla sicurezza dello Stato, conservazione di oggetti di particolare valore) e con precise garanzie (verifica preliminare dell'Autorità, no ad archivi centralizzati, codice cifrato dell'impronta memorizzato solo nel badge del dipendente).
- **Comunicazioni tra amministrazione scolastica e lavoratore:**
  specifiche disposizioni legislative o regolamentari individuano i casi in cui l'amministrazione scolastica è legittimata a comunicare a terzi, soggetti pubblici o privati, informazioni che riguardano i propri lavoratori. Per prevenire la conoscenza ingiustificata di dati da parte di persone non autorizzate, l'amministrazione scolastica deve adottare forme di comunicazione con il dipendente protette e individualizzate, inoltrando le note in busta chiusa, inviandole all'e-mail personale o invitandolo a ritirare personalmente la documentazione.
- **Dati idonei a rivelare le convinzioni religiose:**
  analoghe cautele devono essere osservate nel trattamento di altre tipologie di informazioni sensibili relative al lavoratore, quali quelle idonee a rivelarne le convinzioni religiose. Il trattamento di queste informazioni deve ritenersi in via generale lecito soltanto ove risulti indispensabile per la gestione, da parte dell'amministrazione scolastica, del rapporto di lavoro e, in particolare, per consentire l'esercizio delle libertà religiose riconosciute

ai lavoratori appartenenti a determinate confessioni, in conformità alle disposizioni di legge e di regolamento che regolano i rapporti tra lo Stato e le medesime confessioni.

DIRETTIVA DEL M.I.U.R. N. 104 DEL 30 NOVEMBRE 2007
*("LINEE GUIDA PER LA TUTELA DELLA PRIVACY")*

***"Linee di indirizzo e chiarimenti interpretativi ed applicativi in ordine alla normativa vigente posta a tutela della privacy, con particolare riferimento all'utilizzo di telefoni cellulari o di altri dispositivi elettronici nelle comunità scolastiche".***

AMBITO SOGGETTIVO: la Direttiva si applica ai comportamenti di tutti i soggetti che operano all'interno della comunità scolastica (alunni, personale docente e non docente, altri operatori scolastici) e persegue l'obiettivo di **contrastare abusi e prassi di utilizzo non corretto di telefoni cellulari o di altri dispositivi elettronici** che consentono di acquisire e divulgare immagini, filmati e registrazioni vocali. In altri termini, la Direttiva riguarda i comportamenti dei soggetti che interagiscono dentro la comunità scolastica come "privati"; resta fuori dalla sua applicazione tutto ciò che è riconducibile allo svolgimento di attività didattiche, formative o di apprendimento.

DIVULGAZIONE DEI DATI: la diffusione e/o la comunicazione sistematica di dati personali quali filmati, foto, registrazioni audio ecc. , possono avvenire solo alle seguenti condizioni:

- che la persona interessata (quella ripresa o fotografata) venga **previamente informata** in ordine alle modalità di utilizzo dei dati, con particolare riferimento all'eventualità che i dati siano diffusi o comunicati sistematicamente;
- che la persona interessata abbia **manifestato il suo consenso** (per iscritto se il trattamento riguarda dati sensibili), fermo restando il divieto assoluto di divulgare dati sulla salute.

USO PERSONALE DEI DATI: nelle ipotesi di "uso per fini esclusivamente personali" dei dati acquisiti (filmati, immagini e suoni), non sussistono obblighi particolari per chi li acquisisce, in quanto essi restano nella sua sfera personale o familiare; la condizione è che i dati raccolti **non siano destinati ad una comunicazione sistematica o alla diffusione** e che rimangano in un ambito circoscritto di conoscibilità.
Anche chi utilizza i dati sopra indicati per fini personali deve comunque rispettare **l'obbligo di mantenere sicure le informazioni raccolte** e, se cagiona a terzi un eventuale danno, lo deve risarcire se non prova di avere adottato tutte le misure idonee ad evitarlo.

REGOLAMENTO D'ISTITUTO E SANZIONI DISCIPLINARI: i piani di intervento della Scuola sono diversi e si aggiungono ai profili sanzionatori e risarcitori sopra specificati. Il primo livello di intervento concerne il Regolamento d'Istituto, nell'ambito del quale occorre prevedere le **fattispecie** a cui sono connesse le **sanzioni disciplinari** a carico dei trasgressori, in linea con le indicazioni della Direttiva.
La Direttiva vuole perseguire il fine di favorire la consapevolezza dell'importanza del diritto alla protezione dei dati personali nell'ordinamento vigente, nell'ottica della diffusione della cultura della legalità.

PROVVEDIMENTO GENERALE DEL GARANTE DEL 27 NOVEMBRE 2008
*("Misure e accorgimenti prescritti ai Titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di Amministratore di Sistema")*

DISCIPLINA DELLE FUNZIONI DI AMMINISTRATORE DI SISTEMA: ai sensi dell'art. 154, comma 1, lett. h), il Garante segnala a tutti i titolari di trattamenti di dati personali effettuati con strumenti elettronici la particolare criticità e delicatezza del ruolo dell'Amministratore di Sistema, richiamando l'attenzione dei medesimi titolari sulla necessità di **adottare le seguenti misure ed accorgimenti** idonei a prevenire e ad accertare eventuali accessi non consentiti ai dati personali:

**a) valutazione delle caratteristiche soggettive**
l'attribuzione delle funzioni di Amministratore di Sistema deve avvenire previa valutazione delle caratteristiche di esperienza, capacità ed affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

**b) designazione individuale**
la designazione quale Amministratore di Sistema deve essere individuale e recare l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

**c) identificazione dell'Amministratore di Sistema**
gli estremi identificativi dell'Amministratore di Sistema, con l'elenco completo delle funzioni ad esso attribuite, devono essere riportati nel Documento Programmatico sulla Sicurezza;

**d) verifica delle attività dell'Amministratore di Sistema**
l'operato dell'Amministratore di Sistema deve essere oggetto, con cadenza almeno annuale, di una attività di verifica da parte del titolare del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali;

**e) registrazione degli accessi**
devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte dell'Amministratore di Sistema. Le registrazioni (*access log*) devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

## 2. INDICAZIONE DELLE SEDI, DESCRIZIONE DEI LOCALI E DEGLI STRUMENTI CON I QUALI SI EFFETTUANO I TRATTAMENTI DI DATI

### 2.1 RISORSE

Le risorse da proteggere si possono suddividere in tre categorie·

- **Risorse Fisiche** (locali dove sono ubicate le strutture hardware e software che trattano o ospitano banche dati, nonché gli archivi cartacei documentali);
- **Risorse Hardware** (Server di rete, sistemi informatici su cui operano gli incaricati, modem, router, dispositivi di connessione ad internet);
- **Risorse Software** (programmi informatici, software didattici ed applicativi gestionali).

### 2.2 DESCRIZIONE LUOGHI FISICI DEL TRATTAMENTO DEI DATI

L' **archivio deposito** dell'Ufficio di Segreteria è ubicato al 1° piano del plesso di Via Funi 41 ed ospita le banche dati cartacee dell'Istituto scolastico relative agli alunni, al personale direttivo, docente ed ATA, ai genitori, fornitori ed ai soggetti ed enti esterni che entrano in rapporto con la scuola.
Nella stanza del Direttore SGA si trova la **cassaforte a muro dell'Ufficio di Segreteria** contenente le buste con le password e gli user-id, il denaro contante relativo al Fondo Minute Spese del Direttore SGA, le chiavi di riserva delle serrature degli uffici ed altri documenti riservati. La chiave della cassaforte è disponibile soltanto al Direttore SGA, al quale compete la decisione in ordine alla conservazione o custodia del materiale da inserire all'interno della cassaforte stessa.
L'**archivio corrente** cartaceo, contenente gli atti del titolario con i documenti e gli atti ufficiali dell'istituto, è ubicato, per quanto riguarda il Settore della Didattica, presso la stanza secondaria dell'ufficio di segreteria ed è costituito da n. 3 armadi metallici con idonea chiusura a chiave. Presso la stanza principale dell'ufficio di segreteria, dove si trova il Settore del Personale, sono ubicati n. 2 armadi metallici e n. 3 cassettiere contenenti la documentazione concernente lo stato giuridico del personale docente ed ATA, con relativi fascicoli personali; è presente, inoltre, n.1 armadio blindato contenente materiale tecnico-informatico e le copie di tutte le chiavi della Scuola.
**L'Ufficio del Direttore SGA**, sede del Settore Contabile, ospita n. 3 armadi (di cui uno blindato) e n. 1 classificatore metallico contenente la documentazione relativa alla gestione finanziaria e contabile dell'istituto, ivi compresi i documenti relativi alla gestione patrimoniale; vi si trovano custoditi anche tutti i registri obbligatori ufficiali previsti dalla legge e dal D.I. n. 44/2001.
Tutta la documentazione dell'istituto viene classificata e conservata secondo un apposito titolario degli atti d'ufficio.
**L'Ufficio del Dirigente Scolastico** ospita un armadio blindato contenente il Registro del protocollo riservato, gli atti riservati relativi al personale docente, il registro dei verbali delle sedute degli organi collegiali (Consiglio d'Istituto, Consigli di classe, Collegio dei docenti); il suddetto locale ospita anche n. 1 armadio metallico con idonea chiusura a chiave ed **n. 1 cassaforte di sicurezza** per la conservazione e custodia dei documenti riservati di competenza del Dirigente.

FLUSSO DOCUMENTALE DEI DATI

**A. Dati personali in ingresso:** i documenti cartacei in arrivo, dopo essere stati regolarmente protocollati dall'assistente amministrativo addetto, sono sempre consegnati al Dirigente Scolastico che li esamina, destinando al protocollo riservato quelli appartenenti alle tipologie di dati riservati, sensibili o giudiziari e smistando, per relativa competenza, quelli trattati dall'ufficio di segreteria nelle sue articolazioni funzionali ed organizzative.
I documenti ricevuti via fax o consegnati aperti vengono subito recapitati al Dirigente Scolastico, al quale è demandata la valutazione sul loro trattamento e sulla loro destinazione.
**B. Dati personali in uscita:** i documenti in uscita vengono trattati esclusivamente dal personale incaricato, protocollati e predisposti per la spedizione in busta chiusa. I documenti contenenti dati sensibili o giudiziari vengono chiusi in busta chiusa riservata ed inseriti nel plico contenente la lettera di trasmissione, sulla quale viene evidenziata la circostanza della presenza di documentazione riservata.

CONTROLLI SUL FLUSSO DEI DATI IN INGRESSO ED IN USCITA

**Supporti cartacei:** relativamente ai supporti cartacei, i criteri di protezione dei dati debbono essere ricercati nelle seguenti modalità di trattamento:

- qualsiasi documento relativo agli alunni o al personale dipendente, presentato al protocollo, va inserito in apposite cartelline chiuse non trasparenti ed assegnato all'unità organizzativa competente;

- qualsiasi documento che l'istituzione scolastica deve consegnare agli studenti o al personale dipendente va previamente custodito in apposite cartelline chiuse non trasparenti.

Le rubriche telefoniche in utilizzo su supporto cartaceo sono conservate, dopo la consultazione, in un apposito armadio ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non contiene alcun dato personale o riservato. Gli originali dei telefax inviati mediante apparecchio tradizionale sono riconsegnate a colui che ha eseguito o fatto eseguire la trasmissione, avendo cura di porre quale primo foglio il rapporto di trasmissione formato A4 che viene stampato dal fax, con di seguito i fogli contenenti il messaggio.
La Scuola è provvista di apposita apparecchiatura distruggi documenti ubicata presso l'ufficio di segreteria.

### 2.3 ELENCO SISTEMI HARDWARE

SISTEMA INFORMATICO DELL'ISTITUTO

Nel Sistema Informatico dell'Istituto sono state realizzate **N° 5 Reti locali (LAN),** strutturalmente e funzionalmente autonome.

Le quattro strutture informatiche sono così configurate:

1. **Rete Segreteria Amministrativa** (n° 1 PC SERVER di Rete e n° 10 PC ad uso amministrativo);
2. **Rete Laboratorio Multimediale Scuola Secondaria** (n° 1 PC SERVER e n° 24 PC ad uso didattico);
3. **Rete Laboratorio di Informatica Scuola Primaria** (n° 1 PC SERVER e n° 15 PC ad uso didattico);
4. **Rete Laboratorio di Informatica Scuola Secondaria** (n° 1 PC SERVER e n° 16 PC ad uso didattico);
5. **Rete "Laboratorio di Sostegno CTS "** (n° 1 PC SERVER e n° 9 PC ad uso didattico).

Tutte le postazioni di lavoro sono costituite da Personal Computer con microprocessori (CPU) "Intel Pentium Dual Core" di varia potenza ed hard disk di diverse capacità, con sistemi operativi del tipo Windows XP professional e Windows Server 2008.

**1.** La **Rete Segreteria Amministrativa**, ubicata al piano terra delle sede centrale dell'Istituto, è costituita da n. 9 postazioni assegnate al personale amministrativo dell'Ufficio di Segreteria (compreso il DSGA) e collegate ad un Proxy Server di rete; n. 1 postazione informatica è riservata al Dirigente Scolastico ed è ubicata in una stanza attigua agli uffici amministrativi (stanza presidenza).
Le postazioni di lavoro della rete amministrativa sono connesse mediante switch con cablaggio misto UTP e connettori RJ45 con protocollo TCP/IP. Il PC Server (Windows 2008 Server) gestisce il database "SYBASE" relativo all'applicativo ministeriale SISSI IN RETE, gestisce gli account e funge da Server proxy. Il Server SISSI e il Server Proxy si trovano nella stanza ingresso attigua agli Uffici di Segreteria.
Il Router si trova in un Armadio Rack chiuso a chiave con serratura rinforzata. Tutti i computer della rete amministrativa sono dotati di indirizzo IP statico in classe C .
La connettività Internet avviene attraverso un Router con indirizzo IP statico in classe A (l'ingresso della linea dati di tipo ADSL a 7 mega, fornita dal provider "*Wind Infostrada"*, è localizzato nel Laboratorio di Informatica della Scuola Secondaria, che funge da sorgente fisica primaria di connessione ).

**2.** La **Rete Laboratorio Multimediale Scuola Secondaria,** ubicata al 2° piano della sede centrale, è costituita da n. 24 postazioni multimediali ad uso didattico e per lo svolgimento dei corsi di formazione del personale docente. Tutte le postazioni client sono collegate ad un Proxy Server di rete assegnato, con accesso esclusivo e personalizzato, al docente responsabile di laboratorio appositamente designato dal Dirigente Scolastico.
Le postazioni di lavoro della rete didattica sono connesse mediante HUB con cablaggio misto UTP e connettori RJ45 con protocollo TCP/IP
Sono collegate a questa Rete le seguenti postazioni informatiche (punti rete): n° 2 PC in sala docenti, n° 1 PC in postazione "Auditorium" (sala teatro), n° 1 PC in stanza vice-presidenza, i PC ubicati nelle aule (n. 1 per classe) del plesso scolastico di Via Funi 41, per le quali è stato realizzato il cablaggio in rete con il Laboratorio di Informatica della Scuola Secondaria.
Tutti i computer sono dotati di indirizzo IP statico in classe C. La connettività internet avviene attraverso un Router principale diverso da quello della rete amministrativa. La linea dati , di tipo ADSL a 7 mega, (linea portante della Scuola) è fornita dal provider *Wind Infostrada.*

**3.** La **Rete Laboratorio di Informatica Scuola Primaria** , localizzata nel plesso di Via Funi 81, dispone di n. 15 postazioni in rete collegate ad un Server di rete che controlla le singole postazioni client utilizzate dagli alunni della Scuola Primaria e Infanzia.
Nelle aule della Scuola Primaria sono installati n. 17 PC (n. 1 per classe) come postazioni informatiche non collegate in rete; nella Scuola dell'Infanzia è presente n.1 PC utilizzato dai docenti di tutte le sezioni.
La connettività ad internet avviene mediante una linea dati ADSL a 20 mega fornita dal provider *Telecom Italia.*

**4.** La **Rete Laboratorio di Informatica Scuola Secondaria** , ubicata al piano terra della sede centrale, dispone di n. 16 postazioni in rete collegate ad un Server di rete che controlla le singole postazioni client utilizzate dagli alunni della Scuola Primaria e Secondaria.
La connettività di tutte le postazioni (Server e client) ad Internet avviene attraverso un Router con indirizzo IP statico in classe A (linea dati derivata dal Laboratorio di Informatica del 2° piano, su provider *Wind - Infostrada*).

**5.** La **Rete "Laboratorio di Sostegno CTS",** ubicata al 2° piano della sede centrale, dispone di n. 9 postazioni fisse (e di n. 1 PC notebook) collegate ad un Server di rete che controlla le singole postazioni client utilizzate dagli alunni della Scuola Secondaria.
La connettività di tutte le postazioni (Server e client) ad Internet avviene attraverso un Router con indirizzo IP statico in classe A, su provider *Wind Infostrada.*

### 2.4 ELENCO SISTEMI SOFTWARE

SOFTWARE INSTALLATI SUI PC DELL'ISTITUTO

- I personal computer funzionano con vari sistemi operativi, tra cui WINDOWS 'SP2 e 'XP Professional;
- Le applicazioni di tipo gestionale utilizzate sono le seguenti:
  - Per tutte le aree amministrative gestionali: SISSI IN RETE, Open Sissi, SIDI (Pubblica Istruzione);
  - Per il protocollo: Software "TRE S" Protocollo;
  - Per il conto corrente postale: "TRE S" Conto corrente postale;
  - Applicazioni di MICROSOFT OFFICE AUTOMATION;
  - Software antivirus "SOPHOS ANTIVIRUS";
  - Software Firewall "DIGICOM";
  - OFFICE 2007 XP Standard e Professional: pacchetti software Word – Excel – Power Point – Access – Publisher.
- Sistemi di posta elettronica: Outlook, Outlook Express – Software di navigazione sul Web: "Microsoft Internet Explorer"; sistemi software gestionali: Acrobat Reader, Unico online, Entratel, E-Mens, Nero Burning Rom, Pre 96, Win-Zip, Zip-Genius, Java, Inps gestionale, SQL Sybase, Pensioni S7, SAOL.

Sono state regolarmente acquisite le **licenze di uso** dei software gestionali e dei software firewall ed antivirus, la cui relativa documentazione è conservata presso l'Ufficio di Segreteria e nel laboratorio multimediale della Sez.Secondaria.

### 2.5 ELENCO DELLE BANCHE DATI E TRATTAMENTI OPERATI

## 1. Banca dati Alunni:

| | |
|---|---|
| **Dati sensibili e/o giudiziari** | Profilo diagnostico funzionale, scelta della religione, certificazioni e documenti sanitari, riconoscimento di esonero, agevolazioni, certificati medici relativi allo stato di salute, informazioni relative allo stato di disabilità ed all'handicap, documenti e schede di valutazione personali, Schede personali, documenti ed atti che denotano l'appartenenza etnica e razziale, adesione ad associazioni a carattere religioso, filosofico, politico o morale, procedimenti giudiziari di adozione o tutela, pratiche relative alla tutela di minori, pratiche relative all'affidamento di minori ai servizi sociali. |
| **Supporto informatico** | Inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, gestione SISSI e SIDI, statistiche, trasmissione via e-mail e via fax, relazioni osservative. |
| **Sistemi hardware che ospitano l'archivio** | Server (SISSI in rete). Server (SIDI Istruzione). |
| **Sistemi hardware che trattano l'archivio** | Server (SISSI in rete), computers rete amministrativa. |
| **Sistema di backup e frequenza** | Salvataggio dati (backup) su Hard Disk e CD esterni, frequenza giornaliera. |
| **Archivio cartaceo**<br><br>Localizzazione: - UFFICIO SEGRETERIA VIA FUNI 41 (stanza principale) | Schede di valutazione, Schede personali, domande di iscrizione, tabelle degli esiti finali, diplomi di licenza, pagelle,domande di iscrizione e documenti allegati, certificati medici, documentazione sanitaria, documentazione relativa all'handicap, elenchi e graduatorie, trasferimenti e nulla osta, registro delle assenze, fogli notizie, corrispondenza con le famiglie, pratiche infortuni, partecipazione a viaggi d'istruzione ed |

| | |
|---|---|
| - PLESSO AGGREGATO VIA FUNI 81<br>( Sez. Infanzia e Primaria) | uscite didattiche, buoni libro e domande di borse di studio |

## 2. Banca dati Genitori:

| | |
|---|---|
| **dati sensibili e/o giudiziari** | Documentazione sanitaria e medico-legale, domande di buono libri, domande di borse di studio, domande di contributi, separazioni giudiziali, provvedimenti cautelari, deleghe sindacali, adesione a partiti politici, agevolazioni fiscali, sentenze penali di condanna, documenti relativi a procedimenti giudiziari pendenti, adesione a confessioni religiose, adesione a sindacati di categoria, ad associazioni politiche, filosofiche o morali. |
| **Supporto informatico** | Inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, elaborazione elenchi per elezioni interne di OO.CC., gestione SISSI e SIDI, statistiche, trasmissioni via e-mail e via fax. |
| **Sistemi hardware che ospitano l'archivio** | Server (SISSI in rete). Server (SIDI Istruzione). |
| **Sistemi hardware che trattano l'archivio** | Server (SISSI in rete), computers rete amministrativa. |
| **Sistema di backup e frequenza** | Salvataggio dati (backup) su Hard Disk e CD esterni, frequenza giornaliera. |
| **Archivio cartaceo**<br><br>Localizzazione: UFFICIO SEGRETERIA (stanza principale) | Certificati anagrafici, domande di buono libri, domande di borse di studio, domande di contributi, domande di certificati di iscrizione e frequenza, domande di esonero del pagamento della mensa, documenti relativi allo stato civile, domande di trasferimento alunni,, corrispondenza varia, domande di accesso alla documentazione degli organi collegiali, richiesta di diploma di licenza, pratiche infortuni degli alunni, documentazione varia relativa alla carriera scolastica degli alunni. |

## 3. Banca dati Personale Docente:

| | |
|---|---|
| **dati sensibili e/o giudiziari** | Deleghe sindacali, adesione a partiti politici, documenti sanitari e medico-legali, decreti di decadenza dall'impiego per inidoneità, riconoscimento di esonero, agevolazioni, sanzioni disciplinari, sentenze penali di condanna, documenti relativi a procedimenti giudiziari pendenti, adesione a confessioni religiose, adesione a sindacati di categoria, ad associazioni politiche ed economiche. |
| **Supporto informatico** | Inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione fascicolo personale, gestione SISSI e SIDI, statistiche, trasmissioni via e-mail e via fax. |
| **Sistemi hardware che ospitano l'archivio** | Server (SISSI in rete). Server (SIDI Istruzione). |
| **Sistemi hardware che trattano l'archivio** | Server (SISSI in rete), computers rete amministrativa. |
| **Sistema di backup e frequenza** | Salvataggio dati (backup) su Hard Disk e CD esterni, frequenza giornaliera. |
| **Archivio cartaceo** | Fascicoli personali, documenti di variazione dello stato civile, schede personali, attestati di frequenza di corsi di formazione e aggiornamento, documenti di rito per l'assunzione in servizio, certificati del casellario giudiziale, registro assenze e permessi del personale, decreti di congedo e aspettativa, documenti relativi a stati personali, contratti di assunzione, relazioni sul periodo di |

| | |
|---|---|
| Localizzazione: UFFICIO SEGRETERIA (stanza principale) | prova, retribuzione e compensi accessori, adempimenti fiscali, erariali e previdenziali, procedimenti pensionistici, pratiche di riscatto, anagrafe delle prestazioni, dichiarazione dei servizi e ricostruzioni di carriera. |

## 4. Banca dati Personale ATA:

| | |
|---|---|
| **dati sensibili e/o giudiziari** | Adesione a sindacati, deleghe sindacali, documentazione medico-sanitaria, certificati medico-legali relativi allo stato di salute, diagnosi, riconoscimento di esonero, decreti di congedo e aspettativa per infermità, informazioni relative allo stato di disabilità ed all'handicap, decreti di decadenza dall'impiego per inidoneità, sentenze penali di condanna, documenti relativi a procedimenti giudiziari pendenti, adesione a confessioni religiose, ad associazioni filosofiche , politiche o morali, adesione a sindacati di categoria. |
| **Supporto informatico** | Inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione fascicolo personale, gestione SISSI e SIDI, statistiche, trasmissioni via e-mail e via fax. |
| **Sistemi hardware che ospitano l'archivio** | Server (SISSI in rete). Server (SIDI Istruzione). |
| **Sistemi hardware che trattano l'archivio** | Server (SISSI in rete), computers rete amministrativa. |
| **Sistema di backup e frequenza** | Salvataggio dati (backup) su Hard Disk e CD esterni, frequenza giornaliera. |
| **Archivio cartaceo**<br><br>Localizzazione: UFFICIO SEGRETERIA (stanza principale) | Fascicoli personali, schede individuali, attestati di frequenza di corsi di formazione e aggiornamento, documenti vari, certificati e dichiarazioni varie in entrata ed in uscita, registro assenze e permessi del personale, decreti di congedo e aspettativa, stati personali, contratti di assunzione, documenti di rito, relazioni sul periodo di prova, retribuzioni, schede fiscali, pratiche fiscali, assistenziali e previdenziali, procedimenti pensionistici, pratiche di riscatto e ricongiunzione, anagrafe delle prestazioni, dichiarazione di servizi e ricostruzioni di carriera. |

## 5. Banca dati Soggetti Esterni che prestano opera di collaborazione con la scuola:

| | |
|---|---|
| **dati sensibili e/o giudiziari** | Appartenenza ad enti a carattere filosofico, politico o morale, adesione a confessioni religiose, adesione a sindacati di categoria, ad associazioni politiche ed economiche, adesione a collegi ed ordini professionali, documentazione sanitaria e certificati medico-legali, certificazione antimafia, sentenze penali di condanna, esistenza di procedimenti penali pendenti, documenti che denotano l'appartenenza etnica o razziale. |
| **Supporto informatico** | Inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione SISSI e SIDI, statistiche, trasmissioni via e-mail e via fax. |
| **Sistemi hardware che ospitano l'archivio** | Server (SISSI in rete). Server (SIDI Istruzione). |
| **Sistemi hardware che trattano l'archivio** | Server (SISSI in rete), computers rete amministrativa. |
| **Sistema di backup e frequenza** | Salvataggio dati (backup) su Hard Disk e CD esterni, frequenza giornaliera. |
| **Archivio cartaceo** | Contratti di prestazione d'opera per attività extracurricolari, attestati professionali, lettere di presentazione e accredito, curriculum personale, schede di rilevazione di competenze, domande di partecipazione a gare, attestati di frequenza di corsi di formazione ed |

| | |
|---|---|
| Localizzazione: UFFICIO DIRETTORE SGA | aggiornamento, certificati e dichiarazioni varie in entrata ed in uscita, fatture commerciali, tabelle di liquidazione dei compensi, documentazione attività negoziale, procedimento contrattuale, adempimenti fiscali, erariali e previdenziali, relazioni conclusive sul lavoro svolto, rendicontazioni varie. |

## 6. Banca dati dei Fornitori ufficiali:

| | |
|---|---|
| **dati sensibili e/o giudiziari** | Appartenenza ad enti a carattere filosofico, politico o morale, adesione a confessioni religiose, adesione a sindacati di categoria, ad associazioni politiche ed economiche, adesione a collegi ed ordini professionali, documentazione sanitaria e certificati medico-legali, certificazione antimafia, sentenze penali di condanna, esistenza di procedimenti penali pendenti, documenti che denotano l'appartenenza etnica o razziale. |
| **Supporto informatico** | Inserimento dati, lettura e stampa di dati, variazione di dati, cancellazione di dati, rilascio certificati vari, gestione SISSI e SIDI, statistiche, trasmissioni documenti via e-mail e via fax. |
| **Sistemi hardware che ospitano l'archivio** | Server (SISSI in rete). Server (SIDI Istruzione). |
| **Sistemi hardware che trattano l'archivio** | Server (SISSI in rete), computers rete amministrativa. |
| **Sistema di backup e frequenza** | Salvataggio dati (backup) su Hard Disk e CD esterni, frequenza giornaliera. |
| **Archivio cartaceo**<br>Localizzazione: UFFICIO DIRETTORE SGA | Preventivi per appalti e forniture, contratti di prestazione d'opera, lettere di presentazione e accredito, curriculum personale, schede personali, domande varie, attestati di frequenza di corsi di addestramento professionale, attestazioni tecniche di affidabilità e competenza, fatture commerciali e ricevute fiscali, tabelle di liquidazione dei compensi, documentazione attività negoziale, procedimento contrattuale, adempimenti fiscali, erariali e previdenziali, relazioni conclusive sul lavoro svolto, rendicontazioni contabili varie, convenzioni ed accordi di natura tecnica ed economica. |

## 3. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

### 3.1 COMPITI DELLE SINGOLE FIGURE PREVISTE DALLA NORMATIVA A PROTEZIONE DEI DATI PERSONALI NEL SETTORE DELLA SICUREZZA E LORO NOMINA

### 3.2 IL TITOLARE DEL TRATTAMENTO DEI DATI

Titolare del trattamento dei dati personali è l'Istituto Comprensivo "A. Leonori", rappresentata legalmente pro-tempore dal **Dirigente Scolastico** nella persona della ***Dott.ssa Lina Porrello;***
E' onere del Titolare individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati che assicurino e garantiscano che vengano adottate le misure di sicurezza previste dell'art. 29 del D. Lgs. n. 196/2003. Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure idonee a ridurre al minimo il rischio di distruzione dei dati, l'accesso non autorizzato o il trattamento non consentito, previe idonee istruzioni fornite per iscritto. In caso di assenza dell'incaricato, a fronte della necessità ed urgenza di trattare dati cui solo questi può accedere, il Titolare impartisce istruzioni scritte al Custode delle password ed al Responsabile circa l'apertura della busta contenente i codici di autenticazione e per provvedere ad individuare un altro incaricato.

Ai sensi dell'art.13 del *Codice,* il Titolare ha provveduto a notificare idonea **Informativa** a tutti i soggetti che rivestono la qualità di **interessati al trattamento dei dati personali**, quali sono gli alunni, i dipendenti in servizio presso l'Istituto, i fornitori e gli enti esterni. Scopo dell'informativa è quello di far conoscere agli interessati quali sono i diritti, le finalità, le modalità di trattamento e le garanzie che la legge prevede a tutela della riservatezza delle persone che a vario titolo partecipano alla vita della comunità scolastica.

E' stata data conoscenza pubblica dell'entrata in vigore del nuovo "*Regolamento sul trattamento dei dati sensibili e giudiziari"* mediante pubblicazione all'Albo dell'Istituto delle seguenti informative:

a) **Informativa per il trattamento dei dati personali degli alunni e delle loro famiglie;**
b) **Informativa per il trattamento dei dati del personale dipendente.**

Il *Regolamento* garantisce la tutela delle persone di fronte all'indebito trattamento dei dati, nel rispetto dei principi di correttezza, liceità e trasparenza, con richiamo ai diritti degli interessati.

### 3.3 IL RESPONSABILE DEL TRATTAMENTO DEI DATI

In relazione all'attività del Titolare del trattamento, è prevista la nomina di un **Responsabile del trattamento dei dati**, individuato tra i soggetti che per esperienza, capacità personale ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ai sensi dell'art. 29 del *Codice*.
Il Titolare del trattamento dei dati deve informare il Responsabile delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D. Lgs. n. 196/2003.

Il Responsabile del trattamento dei dati deve svolgere i seguenti **compiti**:
**1**. Redigere ed aggiornare, ad ogni variazione, l'elenco dei sistemi di elaborazione connessi in rete pubblica, nonché l'elenco delle tipologie dei trattamenti effettuati.
**2**. Attribuire, con l'ausilio dell' Amministratore di Sistema (responsabile tecnico della rete informatica), ad ogni incaricato un *codice identificativo personale (USER-ID)* ed una *password* per l'utilizzazione dell'elaboratore, che deve essere individuale e non riutilizzabile.
**3**. Autorizzare i singoli incaricati ad uno specifico trattamento o ad un insieme di trattamenti; qualora si utilizzino elaboratori accessibili in rete disponibili al pubblico, saranno oggetto di autorizzazione anche gli strumenti da utilizzare.
**4**. Verificare, con l'ausilio dell'Amministratori di Sistema, con cadenza almeno quadrimestrale, l'efficacia dei programmi di protezione ed antivirus, nonché definire le modalità di accesso ai locali.
**5**. Garantire che tutte le misure di sicurezza riguardanti i dati in possesso dell'istituzione scolastica siano applicate.
**6**. Informare il Titolare nella eventualità che si siano rilevate nuove tipologie di rischio.
**7**. Adottare tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvedere alla conservazione periodica degli stessi con il sistema di salvataggio mediante idonee procedure di back-up.

La nomina del Responsabile del trattamento deve essere effettuata con **lettera di incarico** e deve essere controfirmata dall'interessato per accettazione; copia della lettera di nomina deve essere conservata a cura del Titolare in luogo sicuro. La nomina è a tempo indeterminato, ma può essere revocata in qualsiasi momento dal Titolare del trattamento dei dati senza preavviso ed eventualmente affidata ad altro soggetto idoneo.

L'Ente titolare del trattamento dei dati personali ha designato, mediante formale atto di nomina, quale **Responsabile del trattamento dei dati** ai sensi dell'art. 29 del *D .Lgs n. 196/2003*, il ***Sig. Dieli Carmelo Roberto***, preposto alle funzioni di Direttore SGA, in considerazione della esperienza, capacità ed affidabilità espressa dal medesimo, tale da offrire idonea garanzia del pieno rispetto delle disposizioni normative in materia di trattamento dei dati personali.

Il suddetto Responsabile del trattamento ha ricevuto adeguate istruzioni riguardo:

**a)** all'individuazione ed adozione delle "***misure minime di sicurezza"*** da applicare nell'ambito dell'istituzione scolastica, al fine di salvaguardare la riservatezza, l'integrità, la completezza e la disponibilità dei dati trattati;
**b)** all'esigenza di provvedere, mediante atto scritto, all'individuazione delle unità legittimate al trattamento, per mezzo dei singoli preposti, ovvero di singoli ***incaricati***, ai sensi dell'art. 30 del *D.Lgs. n. 196/2003*, deputati ad operare sotto la diretta autorità del responsabile attenendosi alle istruzioni impartite, fermo restando l'obbligo gravante sul Responsabile di vigilare sul rispetto delle misure di sicurezza adottate;
**c)** all'esigenza di verificare che gli ***obblighi di informativa*** siano stati assolti correttamente, ovvero che sia stato conseguito il consenso degli interessati laddove necessario;
**d)** all'obbligo di collaborare con il titolare nell'adempiere alle richieste avanzate dal **Garante per la protezione dei dati personali** ovvero alle autorità investite dei poteri di controllo ed ispettivi;
**e)** all'attribuzione della competenza ad elaborare e sottoscrivere notificazioni al Garante per la protezione dei dati personali;
**f)** all'obbligo di osservare e far osservare il divieto di comunicazione e diffusione dei dati personali nei casi previsti dalla legge;
**g)** all'opportunità di proporre soluzioni organizzative che consentano un innalzamento dei livelli di sicurezza e di protezione.
Nell'atto di nomina è stato specificatamente individuato **l'ambito del trattamento consentito** e sono state fissate le **modalità e le finalità** del trattamento stesso.
Per effetto dell'entrata in vigore del D.M. 07 Dicembre 2006 n. 305 (*Regolamento sul trattamento dei dati sensibili e giudiziari nel settore dell'istruzione*), il Titolare del trattamento ha proceduto ad **adeguare,** con formale

provvedimento, la nomina del Responsabile del trattamento **alla nuova disciplina in materia di trattamento dei dati sensibili e giudiziari,** richiamando le prescrizioni contenute nel Regolamento e fornendo gli indirizzi per la loro attuazione nei procedimenti amministrativi e nello svolgimento delle attività istituzionali.

### 3.4 IL CUSTODE DELLE PASSWORD

Il Dirigente Scolastico, Titolare del trattamento dei dati personali, deve nominare un **Custode delle password** a cui conferire il compito di **custodire le buste sigillate contenenti le password** per l'accesso ai dati archiviati nei sistemi di elaborazione presenti presso l'istituto.
Il Titolare deve informare il Custode delle password della responsabilità che gli viene affidata in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D.Lgs. n. 196/2003; deve, inoltre, consegnargli una copia di tutte le norme, in vigore al momento della nomina , che riguardano la sicurezza nel trattamento dei dati personali.
Il Custode delle password deve predisporre, per ogni incaricato del trattamento, una **busta chiusa e siglata** sulla quale è indicato il nominativo: all'interno della busta deve essere indicato, a cura dell'incaricato, lo USER-ID utilizzato e la PASSWORD usata per accedere alla banca di dati; le buste con user-id e password devono essere conservate in luogo chiuso e protetto.
La **nomina** del Custode delle password deve essere effettuata con una lettera di incarico, deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare in luogo sicuro. La nomina del Custode delle password è a tempo indeterminato, può essere revocata in qualsiasi momento dal Titolare senza preavviso, ed essere affidata ad altro soggetto.
Il Titolare ha nominato Custode delle password il DSGA **Sig.** ***Dieli Carmelo Roberto***.

### 3.5 L'AMMINISTRATORE DI SISTEMA INFORMATICO

Per il necessario supporto tecnico-specialistico alle attività di trattamento dei dati, limitatamente alla gestione mediante l'utilizzo di apparecchiature informatiche, l'Istituzione Scolastica si avvale della consulenza e dei servizi tecnico-informatici svolti da una struttura privata esterna denominata "NETWORK ORANGE S.R.L", incaricata mediante apposito "***contratto di assistenza e manutenzione di rete***" (contratto di prestazione d'opera ai sensi dell'art. 2222 c.c.), del supporto, dell'assistenza tecnica, della manutenzione e della riparazione degli strumenti informatici dell'istituto.
Il Titolare di detta struttura, nella persona del Sig. IVAN BENAZZI, nato a Roma il 25/08/1949 ed ivi residente in Via Villandro n.16/A, è stato designato quale "**Amministratore di sistema informatico**" in ragione dei requisiti di specializzazione, professionalità ed abilitazione tecnica posseduti.
Il Titolare del trattamento ha provveduto a specificare all'Amministratore di Sistema le reti, gli elaboratori e le banche dati che questo è chiamato a sovrintendere, informandolo delle responsabilità affidategli in relazione a quanto stabilito dal D.Lgs. n. 196/ 2003.
In ottemperanza a quanto previsto dal *Provvedimento generale del Garante della Privacy del 27 novembre 2008,* al punto 2, lett. c), si riporta **l'elenco delle funzioni e dei compiti** assegnati all'Amministratore di Sistema informatico:

- ✓ assicurare la custodia delle credenziali per la gestione dei sistemi di autenticazione e di autorizzazione in uso all'interno dell'Istituto;
- ✓ impostare e gestire un sistema di autenticazione informatica per i trattamenti di dati personali effettuati con strumenti elettronici, conformemente a quanto previsto dai punti da 1 a 10 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- ✓ impostare e gestire un sistema di autorizzazione per gli incaricati dei trattamenti di dati personali effettuati con strumenti elettronici, conformemente a quanto previsto dai punti da 12 a 14 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- ✓ verificare che la Scuola abbia adottato le misure minime di sicurezza per il trattamento dei dati personali, previste dall'art. 34 del D. Lgs. n. 196/2003, e dal disciplinare tecnico, allegato B) al decreto legislativo medesimo, consigliando il titolare della stessa sugli adeguamenti eventualmente necessari;
- ✓ suggerire al titolare del trattamento l'adozione e l'aggiornamento delle più ampie misure di sicurezza atte a realizzare quanto previsto dall'art. 31 del D. Lgs. n. 196/2003, che dispone che i dati personali oggetto di trattamento devono essere custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- ✓ curare, su incarico del titolare del trattamento, l'adozione e l'aggiornamento delle misure "idonee" di cui al punto precedente;
- ✓ attivare e aggiornare, con cadenza almeno semestrale, idonei strumenti elettronici atti a proteggere i dati trattati

attraverso gli elaboratori del sistema informativo, contro il rischio di intrusione e contro l'azione dei virus informatici;

- ✓ aggiornare periodicamente, con frequenza almeno annuale (*oppure* semestrale *se si trattano dati sensibili o giudiziari*), i programmi volti a prevenire la vulnerabilità degli strumenti elettronici e a correggerne i difetti;
- ✓ impartire a tutti gli incaricati istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale;
- ✓ adottare procedure per la custodia delle copie di sicurezza dei dati e per il ripristino della disponibilità dei dati e dei sistemi (operazioni di *backup e recovery*);
- ✓ predisporre ed aggiornare, entro il 31 marzo di ogni anno, il documento programmatico sulla sicurezza previsto dal punto 19 del Disciplinare tecnico, allegato B) al D. Lgs. n. 196/2003;
- ✓ predisporre un piano di controlli periodici, da eseguirsi con cadenza almeno annuale, dell'efficacia delle misure di sicurezza adottate nella scuola;
- ✓ predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione ed agli archivi elettronici da parte di codesta Società in qualità di Amministratore di Sistema. Le registrazioni *(access log)* devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste; devono altresì comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo di tempo, non inferiore a 6 mesi.

La **nomina** è stata effettuata con apposita **lettera di incarico**, controfirmata dall'interessato per accettazione.
La nomina dell' Amministratore di sistema ha durata annuale, ma può essere revocata dal Titolare del trattamento in caso di gravi inadempienze, per essere affidata ad altro soggetto.

### 3.6 GLI INCARICATI DEL TRATTAMENTO

Al Titolare o al Responsabile del trattamento è affidato il compito di nominare, con comunicazione scritta, uno o più **Incaricati del trattamento dei dati**. La nomina di ciascun incaricato del trattamento dei dati deve essere effettuata con una lettera di incarico in cui sono specificati i compiti affidati (**profilo di autorizzazione**). La nomina deve essere controfirmata dall'interessato per accettazione e copia della lettera di nomina deve essere conservata a cura del Titolare in luogo sicuro.
Gli incaricati del trattamento devono ricevere idonee ed analitiche **istruzioni scritte**, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti. Agli incaricati del trattamento il Responsabile del trattamento deve consegnare una copia di tutte le norme (linee guida) che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.
La nomina degli incaricati è a tempo indeterminato, può essere revocata in qualsiasi momento dal Responsabile per giustificato motivo, senza preavviso, ed essere affidata ad altro soggetto.

Gli incaricati, in particolare, devono essere **informati** in merito alla circostanza che:
**a)** il trattamento e la conservazione dei dati deve avvenire esclusivamente **in modo lecito** e proporzionato alle funzioni istituzionali, nel rispetto della riservatezza delle persone;
**b)** la raccolta, registrazione ed elaborazione dei dati, mediante strumento informatico o cartaceo, deve essere **limitata alle finalità istituzionali**, che sono quelle relative all'istruzione ed alla formazione degli alunni;
**c)** costituisce onere dell'incaricato l'esame e la valutazione della loro **pertinenza** rispetto alle funzioni istituzionali.

L'ambito dei trattamenti autorizzati ai singoli incaricati è suscettibile di aggiornamento periodico.
Il Responsabile del trattamento, ai sensi dell'art. 30 del *D.Lgs. n. 196 /2003,* ha provveduto ad individuare e **nominare** gli **ASSISTENTI AMMINISTRATIVI** **incaricati del trattamento di dati personali**, autorizzandoli al trattamento dei dati in possesso dell'Istituzione Scolastica, esclusivamente con riferimento all'espletamento delle funzioni istituzionali ad essi assegnate dal profilo professionale di appartenenza e secondo quanto previsto dal Piano delle attività del personale ATA.
Per effetto dell'entrata in vigore del D.M. 07 Dicembre 2006 n. 305 (*Regolamento sul trattamento dei dati sensibili e giudiziari nel settore dell'istruzione*), il Responsabile medesimo ha **aggiornato**, con formale provvedimento, le nomine degli Incaricati del trattamento **alla nuova disciplina in materia di trattamento dei dati sensibili e giudiziari**, richiamando le prescrizioni contenute nel Regolamento e fornendo gli indirizzi per la loro attuazione nei procedimenti amministrativi e nella gestione delle attività istituzionali.

Il Titolare ha inoltre provveduto, con apposito atto di nomina personale, alla individuazione dei **docenti incaricati di compiere operazioni di trattamento dei dati personali** nell'espletamento delle funzioni istituzionali e degli incarichi a loro affidati nell'ambito del POF d'istituto per l'a. s. 2010/11.

A tutti gli incaricati autorizzati al trattamento di dati mediante strumenti elettronici sono state conferite **credenziali di autenticazione** (art. 34, comma 1, lett. b) conformi alle caratteristiche indicate nell'allegato B.
Le suddette credenziali sono disattivate automaticamente dal gestore della rete periodicamente, ovvero in tutti i casi di mancata utilizzazione per almeno 3 mesi.

### 3.7 STRUTTURE PREPOSTE AI TRATTAMENTI E RIPARTO DELLE RESPONSABILITA'

Fa parte integrante del presente documento la seguente **mappa delle strutture** con i riferimenti agli incarichi conferiti, ai trattamenti operati ed ai relativi compiti e responsabilità.

| Struttura | Titolare | Trattamenti operati | Compiti |
|---|---|---|---|
| 1 - Dirigente Scolastico | Nominativo:<br>***dott.ssa Lina Porrello*** | Tutti i dati in possesso dell'istituzione scolastica | Direzione generale di tutte le attività; gestione delle pratiche riservate d'ufficio. |
| 2.1 - Collaboratori del Dirigente Scolastico<br><br>2.2 - Coordinatori didattici delle Sezioni | Nominativi:<br>***prof. ssa Ciai Giuliana***<br>*(con funzione vicaria)*<br>***prof.ssa Atzeni Giuliana***<br><br>***Ins. Mancini Marilena***<br>***Ins. Lavatore Giuliana*** | Tutti i dati personali di docenti ed alunni | Supporto organizzativo al DS, con delega di firma e sostituzione del medesimo in caso di assenza o impedimento.<br><br>Gestione personale per assenze, sostituzioni e recuperi. Orario di servizio, adattamenti orario scolastico per gli alunni |
| 3 – Segreteria Amm. va | D.S.G.A.<br>***Dieli Carmelo Roberto*** | Tutti i dati personali dei docenti e del personale amministrativo. | Coordinamento delle attività amministrative e contabili, con responsabilità sul trattamento di tutti i dati personali dell'istituto. |
| 4 - Corpo docente (in organico) | Tutti i ***docenti*** della scuola dell'Infanzia, Primaria e Secondaria di 1° grado. | Tutti i dati personali trattati dai docenti, relativamente ad alunni, genitori e famiglie. | Insegnamento, conduzione di laboratori, orientamento, partecipazione a commissioni varie ed ai lavori degli Organi Collegiali di Scuola |
| 4.1 - Docenti con incarichi specifici per il trattamento dei dati sensibili:<br><br>Docenti di sostegno (in organico) | Tutti i ***docenti di sostegno*** della scuola dell'Infanzia, Primaria e Secondaria di 1° grado. | Dati sensibili relativi ad alunni portatori di handicap. | Partecipazione ai Consigli di classe, GLH d'istituto e GLH operativi.<br><br>Trattamento dei dati personali e sensibili degli alunni |
| 5- Assistenti amministrativi (Profili di autorizzazione) | Nominativi:<br>***1. Colazingari Giovanna***<br>***2. Coppotelli Elisabetta***<br>***3. D'Orio Stefania***<br>***4. Mannarino Fiorella***<br>***5. Moscuzza Luisa***<br>***6. Violante Maria Rosaria*** | Operazioni di trattamento dei dati connesse allo svolgimento di tutte le funzioni amministrative, con particolare attenzione alla tutela dei dati sensibili e giudiziari. | Funzioni amministrative relative alle seguenti Aree:<br>1. Area del Personale<br>2. Area Didattica<br>3. Area Contabile |
| Organi Collegiali<br><br>Membri di diritto | ***Presidenti degli organi collegiali*** | Tutti i dati trattati in fase di elaborazione ed esecuzione delle delibere del Cons. di | Partecipazione alle attività gestionali; decisioni di tipo amministrativo, finanziario, |

| | | | | |
|---|---|---|---|---|
| dei Consigli di Classe, Interclasse , Intersezione | | Classe/Interclasse/Intersezione, Collegio dei Docenti, Organo di Garanzia della Scuola | regolamentare; pratiche disciplinari riguardanti gli alunni ed il personale. | |
| Servizi strumentali all'attività del Consiglio d'Istituto e della Giunta Esecutiva | Soggetto individuato come Responsabile:<br><br>DSGA | Soggetto autorizzato al trattamento dei dati | Trattamenti strumentali alle attività degli organi collegiali ed attività connesse ai rapporti con enti pubblici e privati<br><br>(convocazione degli organi collegiali ed attività di esecuzione delle delibere) | Come sopra |
| Servizi tecnico-strumentali affidati all'esterno, concernenti *l'assistenza e la manutenzione degli strumenti elettronici* (elaboratori e programmi software) | soggetto qualificato come Responsabile:<br><br>*Amministratore di sistema*<br><br>***Sig. Benazzi Ivan***<br><br>***(ditta NETWORK ORANGE s.r.l.)*** | soggetti autorizzati al trattamento dei dati, qualificati come incaricati | Trattamenti strumentali (interventi di carattere tecnico aventi ad oggetto gli strumenti elettronici, effettuati anche al di fuori dei locali di pertinenza dei singoli istituti scolastici)<br><br>Assistenza tecnica e manutenzione delle apparecchiature hardware e software | Come sopra |
| Servizi tecnico-strumentali affidati all'esterno, concernenti lo svolgimento del *Servizio di Cassa relativo alla gestione contabile* dell'istituto | Soggetto qualificato come Responsabile:<br><br>***Banca di Credito Cooperativo di Roma*** | Soggetto autorizzato al trattamento dei dati della scuola nei limiti delle operazioni necessarie per lo svolgimento delle attività conferite<br><br>Trattamento di *dati comuni* | Esecuzione degli ordini di incasso e pagamento emessi dalla scuola nello svolgimento dell'attività contabile di gestione del bilancio<br><br>Lavorazione delle reversali di incasso e dei mandati di pagamento emessi dalla scuola | Servizio di Cassa connesso al Conto Corrente Bancario |
| Servizi tecnico-strumentali affidati all'esterno, concernenti lo svolgimento del *Servizio di Conto Corrente Postale* | Soggetto qualificato come Responsabile:<br><br>***Poste Italiane*** | Soggetto autorizzato al trattamento dei dati della scuola nei limiti delle operazioni necessarie per lo svolgimento delle attività conferite<br><br>Trattamento di *dati comuni* | Gestione delle somme accreditate sul c/c postale della scuola da parte degli alunni per il pagamento del contributo volontario e delle altre somme di denaro dirette a finanziare le gite scolastiche e le altre attività extracurricolari (musicali, teatrali, culturali, sportive, ricreative) | Servizio del Conto Corrente Postale |

## 1. ANALISI DEI RISCHI CHE INCOMBONO SUI DATI PERSONALI

**L'analisi dei rischi** consente di acquisire consapevolezza e cognizione del livello di esposizione al pericolo del proprio patrimonio informativo e di configurare una mappa preliminare d'insieme delle possibili e idonee **contromisure** da adottare.

L'analisi dei rischi consiste nella:

- individuazione di tutte le **risorse** del patrimonio informativo;

- identificazione delle **minacce** a cui tali risorse sono sottoposte;
- identificazione delle **vulnerabilità del sistema**;
- definizione delle relative **contromisure specifiche** da adottare.

Per individuare in concreto i rischi occorre analizzare due diverse dimensioni:
- le possibili **minacce** che possono essere condotte contro il sistema di gestione dei dati personali;
- gli eventuali **punti critici** dello stesso.

Dall'incrocio e dalla combinazione di queste due dimensioni si possono prevedere i pericoli e quindi determinare **strategie ed accorgimenti di natura tecnica ed organizzativa** per ridurli al massimo.

### 4.1 NOZIONI GENERALI

I *requisiti generici di sicurezza* dei sistemi di gestione dei dati presentano le seguenti caratteristiche interdipendenti:

**1) Disponibilità**: i dati devono essere accessibili e i servizi ripristinabili anche in caso di interruzioni dovute alla cessazione dell'alimentazione elettrica, a catastrofi naturali, eventi imprevisti o ad attacchi di pirateria informatica.

**2) Autenticazione**: verifica dell'identità dichiarata da un utente.

**3) Integrità**: controllo che i dati trasmessi, ricevuti o conservati siano completi e inalterati.

**4) Riservatezza**: protezione dei dati trasmessi o conservati per evitarne l'intercettazione e la lettura da parte di persone non autorizzate. La riservatezza è particolarmente necessaria per la trasmissione di dati sensibili ed è uno dei requisiti che garantiscono il rispetto della sfera privata dei loro titolari.

Le *minacce ai dati* possono essere portati dalle seguenti principali **categorie di soggetti**:

– ***Hacker:*** è l'informatico di grande esperienza e competenza, che ha una conoscenza profonda del funzionamento e della struttura dei sistemi informatici. In particolare, l'hacker entra nei sistemi informatici altrui per dimostrare la propria abilità tecnica, per arrecare un danno o per sottrarre informazioni in maniera subdola;

– ***Cracker:*** è l'informatico esperto che si introduce nei sistemi con scopi distruttivi per un interesse personale;

– ***Lamer:*** è un hacker dilettante che è in grado di danneggiare i sistemi informatici con attacchi mirati a singole parti ;

– ***Script Kiddie***: nella pratica informatica è il ragazzino degli Scripts, ovvero un superdilettante, che con strumenti preconfezionati trovati in rete può provocare rilevanti danni. Nella maggior parte dei casi, gli attacchi informatici vengono effettuati da script kiddies che sperimentano tools di hacking recuperati in rete.

### 4.2 RICOGNIZIONE DEI RISCHI

L'Istituzione scolastica ha proceduto ad una ***ricognizione dei rischi*** che potrebbero comportare distruzione, sottrazione, perdita, trattamento abusivo dei dati, sia per effetto di comportamenti di origine dolosa o colposa degli operatori, sia per caso fortuito o forza maggiore.

Le fonti di rischio sono state classificate secondo tre diverse tipologie:

**1) Comportamenti degli operatori:**

Sottrazione di credenziali di autenticazione, comportamenti imperiti, imprudenti o negligenti dei soggetti legittimati al trattamento dei dati, comportamenti dolosi, carenza di consapevolezza, disattenzione o incuria, errori materiali.

**2) Eventi relativi agli strumenti:**

Danno arrecato da virus informatici e/o da hackers, mediante interventi precedenti all'aggiornamento degli strumenti di contrasto attivati (software e firewall), spamming o tecniche di sabotaggio. Malfunzionamento, indisponibilità o usura fisica degli strumenti. Accessi abusivi agli strumenti elettronici. Intercettazione dei dati in occasione di trasmissione in rete.

**3) Eventi relativi al contesto fisico-ambientale:**

Distruzione o perdita di dati in conseguenza di eventi incontrollabili (terremoto) ovvero, seppur astrattamente preventivabili (incendi o allagamenti) di origine fortuita, dolosa o colposa, per i quali non è possibile apprestare cautele. Guasti a sistemi complementari, quale la mancata erogazione di energia elettrica per lunghi periodi di tempo, in grado di pregiudicare la climatizzazione dei locali. Furto o danneggiamento degli strumenti elettronici di trattamento dei dati, in orario diverso da quello di lavoro. Accesso non autorizzato da parte di terzi, interni o esterni all'istituzione scolastica, mediante uso abusivo di credenziali di autenticazione, in funzione di danneggiamento o sottrazione dei dati. Errori umani nell'attivazione degli strumenti di protezione.

### 4.3 PRINCIPALI FONTI DI RISCHIO

Le principali fonti di rischio per la sicurezza e l'integrità nel trattamento dei dati personali sono state individuate nei termini e secondo le classificazioni di seguito rappresentate:

MINACCE A CUI SONO SOTTOPOSTE LE RISORSE HARDWARE

Le principali **minacce alle risorse hardware** sono:

- malfunzionamenti dovuti a guasti e ad anomalie tecniche;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;
- malfunzionamenti dovuti a sabotaggi, furti, intercettazioni (apparati di comunicazione).

MINACCE A CUI SONO SOTTOPOSTE LE RISORSE CONNESSE IN RETE

Le principali **minacce alle risorse connesse in rete** possono provenire dall'interno dell'istituto, dall'esterno o da una combinazione interno/esterno e sono relative:

- all'utilizzo della LAN/Intranet (minacce interne);
- ai punti di contatto con la Rete Internet (minacce esterne);
- allo scaricamento di virus e/o Trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le **seguenti tecniche**:

PACKET SNIFFING:

Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso é possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

PORT SCANNING:

Serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.

HIGHJACKING:

Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione é complessa e richiede elevate capacità e rapidità d'azione.

SOCIAL ENGINEERING:

Apprendimento fraudolento, da parte degli utenti di sistemi di informazioni riservate, sulle modalità di accesso a quest'ultimo.

BUFFER OVERFLOW:

Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che, installate in alcuni sistemi operativi, rivelano le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

PASSWORD CRACKING:

Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine.

TROJAN:

Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.

WORM:

Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).

LOGIC BOMB:

Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione.

MALWARE E MMC (MALICIOUS MOBILE CODE):

Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.

DOS (DENIAL OF SERVICE):

Attacco che mira a saturare le risorse di un servizio, di un server o di una rete.

DDOS (DISTRIBUTED DENIAL OF SERVICE):

Attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete

L'utilizzo di programmi di sniffing e port scanning é riservato esclusivamente all'Amministratore di Sistema per la diagnostica delle prestazioni della rete dell'Istituto; tali programmi non sono in nessun caso utilizzati su reti esterne a quella dell'Istituto.
La lettura in chiaro dei pacchetti in transito può essere autorizzata solo dalla Autorità Giudiziaria ai sensi di legge.

MINACCE A CUI SONO SOTTOPOSTI I DATI TRATTATI

Le **principali minacce ai dati trattati** sono:

- accesso non autorizzato agli archivi contenenti le informazioni riservate (visione, modifica, cancellazione, esportazione) da parte di utenti interni e/o esterni;
- modifiche accidentali (errori, disattenzioni) agli archivi da parte di utenti autorizzati.

MINACCE A CUI SONO SOTTOPOSTI I SUPPORTI DI MEMORIZZAZIONE

Le **principali minacce ai supporti di memorizzazione** sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- l'evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

Ulteriori e più generiche fonti di rischio, o pericoli, per la sicurezza informatica possono essere così classificate:

**Intrusioni:** persone non autorizzate accedono nei locali in cui sono presenti banche dati o penetrano nei sistemi informatici e consultano o alterano o copiano dati o documenti.
*Contromisure*: per i sistemi informatici sono attivabili firewall, proxy server, sistema di account e password; per i luoghi fisici porte con serrature idonee, registri firma e pass di riconoscimento.

**Intercettazione delle comunicazioni:** le comunicazioni elettroniche possono essere intercettate e i dati in esse contenuti copiati o modificati. I punti più vulnerabili e sensibili ad un'intercettazione del traffico sono i punti di gestione e di concentrazione della rete come i *route*r, le *gateway* e i *server* di rete.
*Contromisure*: per i sistemi informatici firewall, proxy server, sistema di account e password; per i luoghi fisici trasporto dei dati sensibili in contenitori con serratura.

**Virus**: sono piccoli programmi che si replicano automaticamente e che possono causare danni di vario tipo. Esempi: *Virus del Kernel (*distruggono il cuore del sistema operativo*), Virus Eseguibile (*possono essere software maligni (malicious software = malware) che modificano o distruggono i dati*), Virus delle Macro* (in Word ed Excel di Microsoft*), Virus del Boot Sector* (si attivano quando si accende il computer e si duplicano sui supporti di memoria*), Bombe Logiche (*rimangono inerti fino al momento in cui vengono innescati da un determinato evento*), Keysniffing* (registra ogni singolo tasto battuto, comprese le password, e le trasmette via Internet).
*Contromisure*: per i sistemi informatici programmi firewall, antivirus e sistema di copie di backup.

**Spyware:** è un software che minaccia la privacy tracciando un profilo sulla base delle navigazioni Internet.
*Contromisure*: per i sistemi informatici programmi di ricerca degli spyware, antivirus, firewall, proxy server.

**Attacchi all'impostazione delle password**: *Brute Force* (un apposito programma prova tutte le possibili combinazioni di chiavi per decrittare il file protetto), *Attacco a Dizionario* (prova lunghissimi elenchi di parole, nomi e sigle di uso comune in una data lingua), *Attacco all'Algoritmo* (prevede la possibilità di intervenire su particolari debolezze matematiche o computazionali dell'algoritmo utilizzato), *Password Sniffing* (ruba la password (sniff) con qualche trucco, facendosela rivelare con un artificio tecnico, o fingendosi responsabile di un servizio assistenza clienti, o della sicurezza)

*Contromisure*: per i sistemi informatici accessi con password elaborate come previsto nel presente documento; per i locali fisici porte con serrature e chiavi custodite in idonee cassette blindate.

**Defacing:** la sostituzione della homepage del sito della scuola con immagini o scritte ingannevoli.
*Contromisure*: sistema di accesso al Server Web con password eUSER –ID.

**Violazione del diritto d'autore:** copie e/o installazioni di programmi informatici di cui la Scuola non possiede regolare licenza; download, illegale e non autorizzato, dal web di file audio e/o video.
*Contromisure*: sistema di autorizzazioni con limitazioni per l'installazione di programmi software, informazione agli utenti, controlli periodici.

**Crimini informatici**: i sistemi informatici della Scuola potrebbero essere utilizzati per compiere crimini informatici con implicazioni di tipo civile e penale: spamming, tentativi di intrusione, pubblicazione sul web di testi o immagini proibite, ecc.
*Contromisure*: sistema di accesso con account e proxy server, in modo tale da impedire alcuni comportamenti illegali ed, in ogni caso, risalire all'autore dell'azione non consentita mediante la tracciatura informatica.

**Danni all'hardware:** l'elemento più delicato è il disco fisso il quale, se si dovesse danneggiare, a meno di ricorrere a pratiche costosissime sviluppate da centri specializzati, tutti i dati andrebbero persi in maniera irrimediabile.
*Contromisure*: nell'ambito del sistema di sicurezza informatica, si procede ad effettuare copie di backup a scadenza periodica e predeterminata.

**Usurpazione di identità:** al momento di stabilire un collegamento alla rete o di ricevere dati, l'utente deduce l'identità del suo interlocutore in funzione del contesto in cui avviene la comunicazione, ma potrebbe scaricare software maligno da un sito *web* che si fa passare per fonte affidabile e si potrebbero anche rivelare informazioni riservate alla persona sbagliata.
*Contromisure*: controllo sistematico dell'autenticità delle fonti di comunicazione.

**IP spoofing:** l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.
*Contromisure*: riservatezza di user-id e password costruite come di seguito indicato.

**Spamming:** saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.
*Contromisure*: software specifico anti-spamming.

**Incidenti ambientali ed eventi imprevisti :** catastrofi naturali (tempeste, inondazioni, incendi, terremoti); opera di terzi estranei a qualsiasi rapporto contrattuale con l'operatore o l'utente (ad es. interruzione dovuta a lavori di costruzione); opera di terzi aventi un rapporto contrattuale con l'operatore o l'utente (ad es. guasti dell'hardware o del software dei componenti o dei programmi consegnati); errore umano dell'operatore (compreso il fornitore del servizio) o dell'utente (ad es. problemi di gestione della rete, installazione errata del software).
*Contromisure*: per i sistemi informatici copie di backup per il ripristino; per i luoghi fisici ricorso a dispositivi di sicurezza e/o armadi dotati di serrature idonee.

### 4.4 VALUTAZIONE DEI RISCHI

Per **valutare i rischi** si utilizzano i seguenti livelli di rilevazione:

**Lieve:** rischio molto basso corrispondente ad una minaccia remota e comunque rapidamente reversibile od ovviabile.
**Medio**: rischio superiore al precedente corrispondente ad una minaccia remota ma i cui effetti non sono facilmente o totalmente reversibili od ovviabili.
**Grave**: rischio che occorre assolutamente prevenire con un insieme di contromisure (di natura fisica, logica, etc..) per abbatterlo e contenerlo in livelli accettabili.

I suddetti livelli di rischio sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione presso l'istituzione scolastica, adottando la seguente scansione:

**A= alto B = basso EE = molto elevato M = medio MA = medio-alto MB = medio-basso**

La tabella seguente sintetizza i principali **eventi potenzialmente dannosi** per la sicurezza dei dati, valutandone le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

**Tabella 4 - Analisi dei rischi**

| EVENTO | | IMPATTO SULLA SICUREZZA DEI DATI | | MISURE DI SALVAGUARDIA |
|---|---|---|---|---|
| | | DESCRIZIONE | GRAVITÀ STIMATA | |
| COMPORTAMENTI DEGLI OPERATORI | Furto di credenziali di autenticazione | Accesso altrui non autorizzato | **M** | Controllo sul rispetto delle prescrizioni normative e tecniche |
| | Carenza di consapevolezza, disattenzione o incuria | Dispersione, perdita e accesso altrui non autorizzato | **M** | Formazione in servizio e flusso continuo di informazione e addestramento professionale |
| | Comportamenti negligenti o fraudolenti | Danni fisici al sistema informatico malfunzionamenti e danni alle risorse hardware | **M** | Vigilanza sul rispetto delle istruzioni e sulle direttive impartite al personale scolastico addetto |
| | Errore materiale | Guasti alle apparecchiature<br><br>Dispersione, perdita, accesso non autorizzato | **M** | Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione |
| EVENTI RELATIVI AGLI STRUMENTI | Azione di virus informatici o di codici malefici | Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori | **EE** | Adozione di idonei dispositivi di protezione e sicurezza informatica<br><br>Software “Firewall”e antivirus |
| | Spamming o altre tecniche di sabotaggio informatico | Danni al sistema operativo, danni al software gestionale, distruzione dei dati | **EE** | Adozione di idonei dispositivi di protezione<br><br>Software “Firewall”e antivirus |
| | Malfunzionamento, indisponibilità o degrado degli strumenti | Alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | **MA** | Assistenza e manutenzione continua degli elaboratori e dei programmi<br><br>Ricambio e sostituzione periodica delle parti soggette ad usura |
| | Accessi esterni non autorizzati | Furto dei dati riservati, attacchi all’impostazione delle password, modifica fraudolenta dei dati | **MA** | Adozione di adeguati dispositivi di vigilanza e protezione dall’esterno |

| | | | | |
|---|---|---|---|---|
| | Intercettazione di informazioni in rete | Dispersione di dati; accesso altrui non autorizzato | **MA** | Installazione di software antivirus ad aggiornamento periodico e controllato |
| **EVENTI RELATIVI AL CONTESTO DEI LUOGHI FISICI** | Accessi non autorizzati a locali/reparti ad accesso ristretto e controllato<br><br>Possibilità di intrusione negli archivi di segreteria e presidenza o in sala docenti | Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori<br><br>Furto di materiale informatico<br><br>Cancellazione non autorizzata di dati o manomissione di apparecchiature tecniche | **M** | Protezione dei locali mediante serratura rinforzata, con distribuzione delle chiavi ai soli autorizzati<br><br>Protezione dei locali mediante sistema di allarme antintrusione con sensori a raggi infrarossi |
| | Asportazione e furto di strumenti contenenti dati personali | Dispersione e perdita di dati, di programmi e di elaboratori; accesso altrui non autorizzato | **MB** | Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati |
| | Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria e negligenza | Cancellazione e distruzione di dati, dei programmi, danni fisici agli elaboratori | **M** | Attività di prevenzione, controllo, assistenza e manutenzione periodica,vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione |
| | Guasto ai sistemi complementari (impianto elettrico, sistema di allarme, climatizzazione, estintori, etc.) | Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | **A** | Installazione di gruppi di continuità<br><br>Attività di controllo, assistenza e manutenzione periodica degli impianti di sicurezza<br><br>Formazione del personale in servizio addetto alla sicurezza ai sensi del D. Lgs.626/94 |
| | Errori umani nella gestione della sicurezza fisica | Furti, manomissione di apparecchiature informatiche, possibilità di sabotaggio, uso fraudolento degli strumenti tecnologici. | **M** | Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione degli addetti |

## 5. MISURE MINIME DI SICUREZZA IDONEE A GARANTIRE L' INTEGRITA', LA PROTEZIONE, LA SALVAGUARDIA ED IL RIPRISTINO DEI DATI.

## 5.1 MISURE DI SICUREZZA CONTRO IL RISCHIO DI DISTRUZIONE O PERDITA DI DATI

In questa parte del documento vengono descritte le **"Misure minime di sicurezza",** previste e disciplinate dal *Capo II – Art. 33 del D.Lgs. n. 196/2003,* adottate per contrastare i rischi individuati a seguito dell'analisi effettuata e della valutazione degli eventi. Per "*misura"* viene inteso lo specifico intervento tecnico, informatico od organizzativo, posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, nonché per assicurare il livello minimo di protezione dei dati personali oggetto di trattamento.
Vengono indicate, altresì, tutte le **contromisure, le attività di verifica e controllo** da porre in essere periodicamente, essenziali per assicurare l'efficacia della protezione ad ogni livello.

ANALISI DEL SISTEMA DELLE CONTROMISURE

Per **contromisure** si intendono le azioni e gli accorgimenti tecnici che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce; esse sono classificabili secondo tre seguenti tre categorie:

A. **contromisure di carattere fisico;**
B. **contromisure di carattere procedurale;**
C. **contromisure di carattere elettronico/informatico.**

### A) CONTROMISURE DI CARATTERE FISICO

In considerazione di quanto disposto dal *D. Lgs. n. 196/2003*, **è fatto divieto a chiunque di:**

- Effettuare copie di dati su supporti magnetici o trasmissioni di dati non autorizzate dal Responsabile o dal Titolare del trattamento dei dati;
- Effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile del trattamento dei dati, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
- Sottrarre, cancellare, distruggere senza l'autorizzazione del Responsabile del trattamento dei dati stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento;
- Consegnare, a persone non autorizzate dal Responsabile del trattamento dei dati, stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento.

- le **apparecchiature informatiche critiche** (Server di rete, computer utilizzati per il trattamento dei dati personali, apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali sono situati presso l'Ufficio di Segreteria dell'istituto in **locali controllati ad accesso controllato**;
- gli **incaricati** responsabili dei trattamenti sono anche **responsabili dell'area** in cui avvengono materialmente i trattamenti;
- sono allo studio ulteriori e più sofisticati interventi atti ad elevare al massimo il livello di protezione e sicurezza dei locali dove sono custoditi i documenti contenenti dati personali (porte corazzate, armadi blindati, impianti elettrici dedicati, sistemi di condizionamento, apparecchiature di continuità elettrica).

PROTEZIONE DEI LOCALI E DELLE AREE IN CUI VENGONO TRATTATI I DATI

Contro i **rischi di intrusione indebita dall'esterno**, i locali sono dotati di **impianto di allarme a sensori infrarossi**, attivabile mediante digitazione di un codice alfanumerico in possesso del collaboratore scolastico che svolge le mansioni di custode. Si predispone l'attivazione di detto sistema di allarme al termine dell'orario di lavoro e delle attività didattiche, al momento della chiusura dei locali dell'edificio scolastico.
Viene assicurata l'esecuzione controllata di **test periodici sull'efficienza del Sistema di allarme.**
Le aree che ospitano documenti contenenti dati personali sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso.
L'ubicazione delle stampanti, delle fotocopiatrici e dell'apparecchio telefax non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale appositamente addetto.
Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare ad ogni variazione l'elenco degli uffici in cui viene effettuato il trattamento dei dati, nominando un apposito incaricato con il compito di controllare direttamente i sistemi, le apparecchiature, o i registri di accesso ai locali, allo scopo di impedire indebite intrusioni o danneggiamenti.
Il Responsabile del trattamento dei dati deve definire **le modalità di accesso agli uffici** in cui sono presenti sistemi o apparecchiature di accesso ai dati trattati, nonché informare con apposita comunicazione scritta l'incaricato dei compiti che gli sono stati affidati, utilizzando un modulo appositamente predisposto.

In materia di Sicurezza sono state recepite le nuove norme di cui al **D. Lgs. 09/04/2008 n. 81 - Testo Unico in materia di tutela della Salute e della Sicurezza nei luoghi di lavoro** (come modificato dal D.Lgs. n. 106/2009), il

quale introduce importanti novità in ordine alla definizione dei contenuti del "Documento di Valutazione dei Rischi", prevedendo in particolare tre nuovi adempimenti:

1. l'individuazione delle **procedure** da adottare per l'attuazione delle misure di sicurezza obbligatorie;
2. l'indicazione, nel documento, dei nominativi del **RSPP e del RLS;**
3. l'individuazione delle **mansioni che espongono i lavoratori a rischi** per i quali è richiesta capacità professionale, specifica esperienza, adeguata formazione ed addestramento.

## B) CONTROMISURE DI CARATTERE PROCEDURALE

- l'ingresso nei locali ad accesso controllato è consentito solo alle **persone autorizzate**;
- il **responsabile dell'area** ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- **i visitatori occasionali** della aree ad accesso controllato, se autorizzati dal Dirigente Scolastico, sono accompagnati da un collaboratore scolastico incaricato;
- per l'ingresso nei locali dell'Ufficio di Segreteria è necessaria preventiva autorizzazione da parte del Responsabile (DSGA) o del Titolare (DS) del trattamento;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli **allarmi e degli estintori**;
- **l'ingresso in locali** ad accesso controllato da parte di dipendenti o estranei, per operazioni di pulizia o di manutenzione, avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono protetti da green-saver, oppure se le operazioni si svolgono alla presenza dell'incaricato del trattamento di tali dati;
- **i Registri di classe**, contenenti dati personali e riservati, durante l'orario delle lezioni sono tenuti in classe sulla scrivania sotto la custodia e la responsabilità dell'insegnante di turno. Al termine delle lezioni vengono conservati in apposito armadio con chiusura a chiave dall'insegnante dell' ultima ora di lezione;
- il docente è responsabile della custodia del **Registro personale** in cui sono annotati dati personali e riservati. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del docente che è chiuso a chiave, con una chiave di riserva che è custodita con le dovute cautele dal Dirigente Scolastico ;
- il **Registro del protocollo riservato**, accessibile solo al Titolare del trattamento è conservato presso la stanza del Dirigente Scolastico, in apposita cassaforte di sicurezza;

  Per il trattamento dei soli **documenti contenenti dati cartacei** sono adottate le seguenti disposizioni:
  - si accede ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
  - si utilizzano archivi con accesso selezionato;
  - atti e documenti devono essere restituiti al termine delle operazioni;
  - è fatto divieto di fotocopiare/scannerizzare documenti senza l'autorizzazione del Responsabile del trattamento;
  - è fatto divieto di esportare documenti o copie dei medesimi all'esterno dell'istituto senza l'autorizzazione del Responsabile del trattamento; tale divieto si estende anche all'esportazione telematica dei dati personali;
  - il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti deve essere ridotto in minuti frammenti, mediante l'utilizzo dell'apposita macchinette distruggi documenti.

## C) CONTROMISURE DI CARATTERE ELETTRONICO/INFORMATICO

Le **misure di carattere elettronico/informatico**[1] adottate sono le seguenti:

- presenza di **gruppi di continuità** elettrica per il Server di rete e per i personal computer utenti;
- attivazione di un **Sistema di Backup e Restore** centralizzato su Server con periodicità giornaliera;
- installazione di un efficace **Software Firewall** con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet;
- definizione delle **regole per la gestione delle password** per i sistemi dotati di sistemi operativi Windows SP2 ed XP;
- installazione di un **Sistema Antivirus** su tutti le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza giornaliera e la scansione periodica dei supporti di memoria;
- definizione delle regole per la gestione degli strumenti elettronici/informatici;
- definizione delle **regole di comportamento** per minimizzare i rischi da virus;

[1] Le *misure di carattere elettronico/informatico* sono quelle in grado di segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, di gestire le copie di salvataggio dei dati e degli applicativi, di assicurare l'integrità dei dati, di proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi.

- separazione della Rete LAN della segreteria amministrativa da quella del laboratorio informatico didattico.

DISPOSITIVI SOFTWARE DI PROTEZIONE DEI DATI

***A) Impostazioni di Windows:*** il primo grande problema di sicurezza è rappresentato dal modo in cui è impostato il sistema operativo (SO). Se, ad esempio, si usa Windows occorre utilizzare la funzione che si chiama "Windows Update". Serve per aggiornare quasi automaticamente il sistema operativo, scaricando dal sito della Microsoft tutte le "patch" di sicurezza necessarie. Una "patch" è un piccolo file che serve per risolvere un problema software. Occorre eseguire la stessa azione per il browser: con Internet Explorer si verifica sul sito della Microsoft l'esistenza di patch di aggiornamento.

***B) Password di screen saver***: è un sistema di protezione che si attiva quando ci si allontana dalla postazione lasciando il computer acceso. Occorre seguire le seguenti istruzioni: Start - Impostazioni – Pannello di Controllo - Schermo; selezionare schermata dello screen saver, spuntare con il flag (segno nero) sul quadratino Protezione; cliccare su Cambia ed inserire una password, infine dare l'ok. La password va cambiata almeno ogni 3 mesi.

***C) Opzioni di sicurezza del Browser:*** impostare il livello di protezione durante la navigazione su livelli medio-alti (per es. con Internet Explorer 5, Strumenti - Opzioni Internet - Protezione – Livello personalizzato - Impostazioni personalizzate e scegliere o media o alta); con Internet Explorer 8 si possono rifiutare i cookies (Strumenti - Opzioni Internet - Privacy - protezione massima o quella immediatamente inferiore).
Per conseguire più elevati livelli di protezione del sistema durante la navigazione, tutte le postazioni Client della Segreteria Amministrativa vanno aggiornate all'ultima versione di Internet Explorer.

***D) Password di apertura e scrittura di Word ed Excel:*** quando si elabora un file con *Word* o *Excel* di Microsoft è possibile associare una password da digitare obbligatoriamente per poterlo leggere e/o modificare (File - Salva con Nome – nella finestra che si apre selezionare Strumenti – Opzioni Generali - scrivere la sequenza in una delle due caselle "password di apertura" e "password di modifica", nel primo caso il documento non può essere aperto, nel secondo caso sarà visibile ma non modificabile).

Il Server è collegato a gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o di interruzione di erogazione di corrente elettrica.
L'Istituzione Scolastica dispone di armadi blindati per la conservazione e archiviazione dei supporti di salvataggio creati precedentemente al nuovo sistema di backup centralizzato, nonché di apposite scrivanie con chiavi. L'introduzione di password all'accensione dei personal computers, di password dello screen-saver e di password per l'accesso in rete determina un livello di sicurezza, circa i dati contenuti nei computers, ritenuto più che soddisfacente ed in regola con la previsione normativa.
Su tutti i personal computer degli utenti e sul Server SISSI è installato il ***Software Antivirus "SOPHOS"*** che viene automaticamente e costantemente aggiornato dal relativo sito INTERNET. Il programma consente di rilevare immediatamente all'apertura di un file la presenza di virus dannoso per il sistema. I virus riconosciuti sono eliminati immediatamente, mentre quelli nuovi vengono messi in quarantena e vanno eliminati dagli operatori mediante scansione periodica da effettuare con cadenza almeno settimanale. Detto software controlla anche le caselle di posta elettronica ed i file di *attach.*
Sulla rete della Segreteria Amministrativa e dei Laboratori di Informatica è installato un ***Software Firewall "DIGICOM"*** idoneo a proteggere il sistema da attacchi ed intrusioni dall'esterno, assicurando elevati livelli di sicurezza informatica. Esso rappresenta una efficace barriera di protezione in grado di monitorare e controllare le informazioni trasmesse tra i singoli client e la rete o Internet.

Si descrivono analiticamente, di seguito, le *caratteristiche tecniche* richieste e le *modalità di funzionamento* dei **sistemi di protezione** necessari per una efficace protezione del sistema informatico:

***SOFTWARE FIREWALL*** ("muro tagliafuoco"): è un software che controlla le connessioni, le porte, i dati in ingresso ed in uscita, bloccando gli accessi e gli invii di dati non autorizzati o sconosciuti; serve a tutelare il sistema informatico durante la navigazione sulla rete internet.
***SERVER PROXY:*** durante la navigazione su Internet, viene attribuito al computer un indirizzo IP, che lo identifica in maniera univoca in tutto la rete Web. Conoscendo l'indirizzo IP è possibile individuare la rete, la sottorete ed il provider a cui si è connessi. Per impedire di essere individuati con tanta precisione, occorre utilizzare un server Proxy.
Un Proxy server è un computer che si interpone fra il proprio computer e Internet, facendo da intermediario per tutto il traffico di dati sia in uscita che in entrata.
In pratica i singoli computer non hanno accesso diretto alla rete esterna, ma solamente il proxy. Il che vuol dire che non saranno le identità dei singoli computer a viaggiare in rete, ma solamente quella del proxy.
***SOFTWARE ANTIVIRUS:*** è un software che controlla sempre tutti i file che vengono introdotti nel sistema informatico, svolgendo un importante funzione di protezione dei dati contenuti nell'elaboratore che si sta utilizzando.

Se un file od un programma appena avviato sembra comportarsi in modo anomalo, occorre bloccarlo e rivolgersi all'Amministratore di Sistema.

## SISTEMA DI AUTORIZZAZIONE INFORMATICA

Il **controllo degli accessi** alle varie postazioni di lavoro viene effettuato mediante l'istituzione di un sistema di autorizzazione che permette l'identificazione indiretta del soggetto autorizzato al trattamento dei dati tramite riconoscimento di una **credenziale di autenticazione** logica, costituita da un "*codice identificativo personale*" (USER-ID) associato ad una "*password*" riservata.
Tutti i computer presenti negli Uffici di Segreteria, compreso il Server, sono utilizzabili tramite digitazione di apposita ***password*** di cui sono a conoscenza esclusivamente gli assistenti amministrativi addetti.
L'attivazione della "condivisione"dei dati contenuti nei client delle varie postazioni di lavoro collegate in rete è limitata solo alle cartelle che non contengono dati personali e riservati.
La consegna delle password agli incaricati del trattamento dei dati viene effettuata in forma riservata, in busta chiusa e con raccomandazione alla custodia. Di dette operazioni viene redatto apposito verbale di consegna da parte del Responsabile del trattamento dei dati.

## REGOLE PER LA GESTIONE DELLE PASSWORD[2]

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo del predetto **codice identificativo personale (in seguito indicato user-id) e password personale**.
User-id e password iniziali sono assegnati dal custode delle password, sono strettamente personali e non possono essere riassegnate ad altri utenti.
La password non può contenere elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una **busta chiusa** al Custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.
Le password verranno automaticamente disattivate dopo 3 mesi di non utilizzo.
In caso di urgente necessità, l'amministratore di sistema è autorizzato a intervenire sui personal computer.
In caso di **manutenzione straordinaria** possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione, le credenziali di autenticazione di accesso. Al termine delle operazioni di manutenzione, l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:

- le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
- per la **definizione/gestione della password** devono essere rispettate le **seguenti regole**:
  - la password deve essere costituita da una sequenza di **minimo 8 caratteri** alfanumerici e non deve essere facilmente individuabile;
  - al primo accesso la password ottenuta dal custode delle password deve essere cambiata; la nuova password non deve essere simile alla password precedente;
  - la password deve essere **cambiata almeno ogni 3 mesi**, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
  - la password è **segreta** e non deve essere comunicata ad altri;
  - la password va custodita con diligenza e riservatezza.

## REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICO/INFORMATICO

Per gli elaboratori che ospitano archivi con dati riservati sono adottate le **seguenti misure**:

- **l'accesso agli addetti alla manutenzione** è possibile solo in seguito ad autorizzazione del Responsabile;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- è fatto divieto, agli utilizzatori di strumenti elettronici, di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno "**screensaver" automatico** dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione, negli archivi informatici, di dati riservati di carattere personale e di dati sensibili non inerenti alla funzione svolta dall'incaricato in relazione alla propria prestazione lavorativa;
- **divieto di installazione di software** di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;

[2] La *password* è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.

- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.

## CRITERI E PROCEDURE PER GARANTIRE LA SICUREZZA NELLA TRASMISSIONE DEI DATI

Al fine di garantire la massima sicurezza nella **Trasmissione telematica dei dati riservati dell'istituto** ad Enti ed Istituzioni pubbliche abilitate per legge a richiedere flussi di informazioni e dati gestionali di natura diversa (fiscale, previdenziale ed assistenziale, contabile ecc), attraverso l'utilizzo di apparecchi di trasmissione quali "Modem" e "Router", il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'amministratore di sistema, le **misure tecniche da adottare** in rapporto al rischio di intercettazione o di intrusione di "hacker" o di "cracker" su ogni sistema collegato in rete pubblica. I criteri debbono essere definiti dall'amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni sistema interessato debbono essere definite le seguenti specifiche:

- Le misure tecnico-informatiche applicate per evitare **intrusioni ed intercettazioni** nella comunicazione;
- Le misure di sicurezza applicate per evitare **contagi da virus informatici**.

## REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS

Per **minimizzare il rischio da virus informatici**, gli utilizzatori dei PC adottano le seguenti precauzioni operative:

- limitare lo scambio fra computer di supporti rimovibili (dvd, cd, chiavi USB) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;
- controllare (**scansionare con un antivirus aggiornato**) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza;
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai su di un link presente in un messaggio di posta elettronica di provenienza sconosciuta, in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat attivate sui siti Internet, neanche su quelli autorizzati;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

## PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire **l'integrità dei dati** contro i rischi di distruzione o perdita **a causa di virus informatici**, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'amministratore di sistema, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.
Il Responsabile del trattamento dei dati stabilisce inoltre la periodicità con cui debbono essere effettuati gli **aggiornamenti dei sistemi antivirus** utilizzati per ottenere un accettabile standard di sicurezza delle banche dati trattati.
I criteri debbono essere definiti dall'amministratore di sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata. In particolare, per ogni sistema debbono essere definite le seguenti specifiche:

- Il tipo di programma utilizzato;
- La periodicità di aggiornamenti;

Per ogni sistema deve essere predisposto apposito **modulo di rilevazione di virus informatico,** sul quale debbono essere annotati eventuali virus rilevati, e se possibile, la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche. I moduli compilati ed aggiornati dagli incaricati

del trattamento debbono essere conservati a cura del Responsabile del trattamento dei dati in luogo sicuro e debbono essere trasmessi in copia all'amministratore di sistema.

INFEZIONI E CONTAGIO DA VIRUS INFORMATICI

Nel caso in cui su uno o più sistemi si dovesse verificare **perdita di informazioni o danni a causa di infezione o contagio da virus informatici,** l'amministratore di sistema deve provvedere a:

- Isolare il virus informatico.
- Verificare se ci sono altri sistemi infettati con lo stesso virus informatico.
- Identificare l'antivirus adatto e bonificare il sistema infetto.
- Installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti.

INCIDENT RESPONSE INFORMATICO E RIPRISTINO

Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno,abuso, compromissione dell'informazione o perdita di beni.
Tutti gli **incaricati del trattamento dei dati** devono avvisare tempestivamente il Responsabile del trattamento dei dati o l'amministratore di sistema, nel caso in cui constatino le seguenti **anomalie**:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In **caso di incidente** sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'amministrazione scolastica.

Garantita **l'incolumità fisica** alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente.
4. documentare tutte le operazioni compiute.

Una volta spento, il sistema oggetto dell'incidente non deve più essere riacceso.

Se l'incidente è dovuto ad imperizia o imprudenza del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.

## 5.2 CRITERI E PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI

Al fine di garantire **l'integrità dei dati contro i rischi di distruzione o perdita**, il Responsabile del trattamento dei dati stabilisce, con il supporto tecnico dell'amministratore di sistema, la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati. I criteri debbono essere definiti dall'Amministratore di Sistema in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata.
In particolare per ogni banca di dati debbono essere definite le seguenti specifiche:

- Il tipo di supporto da utilizzare per le copie di back-up.
- Se per effettuare le copie di back-up si utilizzano procedure automatizzate e programmate.
- L'incaricato del trattamento a cui è stato assegnato il compito di effettuare le copie di backup.
- Le istruzioni e i comandi necessari per effettuare le copie di back-up.

PROCEDURA DI SALVATAGGIO DEI DATI (BACKUP)

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, è stata definita una "**procedura integrata**" di periodica esecuzione di **salvataggio dei dati personali dell'Istituto,** come di seguito rappresentata:
***1.*** BACKUP CENTRALIZZATO SU SERVER DI RETE: è stato adottato un **Sistema Centralizzato** di salvataggio dei dati sul **Server della Rete LAN** dell'ufficio di Segreteria. Gli utenti di rete (assistenti amministrativi incaricati del trattamento dei dati dell'Istituto) salvano i dati elaborati sul proprio PC direttamente sul Server di Rete, tramite una procedura manuale effettuata con cadenza **giornaliera,** utilizzando apposita Cartella di collegamento al Server.

***2.*** SALVATAGGIO DATI SU HARD DISK ESTERNO: sul Server di Rete è stata creata una configurazione di sistema per la esecuzione di una **procedura automatica, a cadenza giornaliera, di salvataggio dei dati** riversati dalle singole postazioni di rete (Client) su un Hard Disk Esterno (da 120Gb espandibile con porta USB) che svolge la funzione di supporto di memorizzazione.
Le operazioni di salvataggio, effettuate nel modo come sopra descritto, sono controllate e verificate con cadenza settimanale dall'Amministratore di Sistema, allo scopo di garantire la conservazione e l'integrità dei dati.
**3.** SALVATAGGIO DATI SU CD-ROM: per conseguire elevati livelli di garanzia nella protezione dei dati personali dell'Istituto, viene adottato anche un sistema di salvataggio dei dati su supporti di memorizzazione di massa (CD ROM) che vengono custoditi in una cassaforte situata nell'Ufficio di Segreteria **(sistema del doppio backup).**

Con riferimento al contenuto ed alle competenze in materia di **copia di sicurezza, verifica e ripristino**, le soluzioni organizzative adottate presso l'istituzione scolastica sono sintetizzate nella seguente tabella:

**Tabella 7 - Salvataggio dei dati (Backup)**

| SALVATAGGIO | | CRITERI INDIVIDUATI PER IL SALVATAGGIO | UBICAZIONE DI CONSERVAZIONE DELLE COPIE | STRUTTURA OPERATIVA INCARICATA DEL SALVATAGGIO |
|---|---|---|---|---|
| STRUTTURA | TIPOLOGIA DI DATI | | | |
| **Ufficio del Dirigente Scolastico** | *Dati personali, sensibili e giudiziari* relativi agli alunni ed al personale docente.<br><br>*Dati riservati* dell'istituzione scolastica (protocollo riservato). | Salvataggio dati giornaliero | HARD DISK ESTERNO SU SERVER DI RETE sito a *Piano terra,* nella stanza principale dell'ufficio di segreteria.<br><br>CD-ROM custoditi in cassaforte Segreteria | Titolare del trattamento<br><br>*Dirigente Scolastico* |
| **Ufficio di Segreteria**<br><br>Area Personale | 1) *Dati sensibili*: Stato di salute (assenze dal servizio, aspettative)<br>- adesione a sindacati<br>- origine razziale o etnica<br>- confessione religiosa.<br><br>2) *Dati giudiziari:* Procedimenti giudiziari civili e penali, certificati del casellario giudiziale. | Salvataggio dati giornaliero (anche esterno all'Istituto) | HARD DISK ESTERNO SU SERVER DI RETE sito a *Piano terra,* nella stanza principale dell'ufficio di segreteria.<br><br>PORTALE SIDI ISTRUZIONE<br><br>**Database nazionale** Istituzioni Scolastiche | Responsabile del trattamento<br><br>*(Direttore SGA)* |

| | | | | |
|---|---|---|---|---|
| **Ufficio di Segreteria**<br><br>Area Contabilità | 1) *Dati contabili* relativi ad alunni e personale scolastico, a fornitori ufficiali e ad imprese interessate ad attività negoziali poste in essere dal D.S. | Salvataggio dati giornaliero (anche esterno all'Istituto) | PORTALE SIDI ISTRUZIONE<br><br>**Database nazionale** Istituzioni Scolastiche | Assistente Amm.vo responsabile pro tempore del servizio |
| **Ufficio di Segreteria**<br><br>Area Alunni<br><br>(*Servizi inerenti all'offerta formativa)* | *1) Dati sensibili e giudiziari:* relativi agli alunni o ai genitori degli alunni. | Salvataggio dati giornaliero | HARD DISK ESTERNO SU SERVER DI RETE sito a *Piano terra,* nella stanza principale dell'ufficio di segreteria.<br><br>CD-ROM custoditi in cassaforte Segreteria | Assistente Amm.vo responsabile pro tempore del servizio |
| **Area Didattica**<br><br>Attività curricolare<br><br>Attività extracurricolare<br><br>(*Servizi strumentali agli organi collegiali)* | *1) Dati sensibili e giudiziari:* relativi agli alunni o ai genitori degli alunni. | Salvataggio dati giornaliero | HARD DISK ESTERNO SU SERVER DI RETE sito a *Piano terra,* nella stanza principale dell'ufficio di segreteria.<br><br>CD-ROM custoditi in cassaforte Segreteria | Docenti con incarico di *Coordinatori di classe* e docenti del sostegno |
| | | | | |

PROCEDURA DI RIPRISTINO DEI DATI (RESTORE)

Viene anche predisposto un **piano di salvaguardia e ripristino**, per combattere il rischio di perdita dei dati in caso di contaminazione dei sofware o malfunzionamento dei sistemi hardware.

Con riferimento alle **procedure di ripristino**, l'istituzione scolastica ha adottato le modalità tecniche raffigurate schematicamente nella seguente tabella:

**Tabella 8 - Ripristino dei dati**

| DATA BASE/ARCHIVIO | SCHEDA OPERATIVA | PIANIFICAZIONE DELLE PROVE DI RIPRISTINO |
|---|---|---|

| | | |
|---|---|---|
| **Servizi Amministrativi**<br>**Ufficio di Segreteria**<br>1. Database" SISSI IN RETE"<br>- Area Nuovo Bilancio<br>(migrata sul Portale SIDI Istruzione)<br>- Area Retribuzioni<br>- Area Personale<br>- Area Alunni<br>- Area Gestione Fiscale<br>- Area Libri di Testo<br>- Area Biblioteca<br>- Area Magazzino<br><br>2. Cartelle Documenti e File contenenti informazioni e dati riservati degli alunni e del personale Docente e ATA | Procedura di Ripristino di tipo MANUALE<br><br>Procedura di Ripristino effettuata dall'Amministratore di Sistema | **Fasi operative di ripristino dei dati**<br><br>1. Formattazione Hard Disk Server.<br>2. Ripristino Sistema Operativo.<br>3. Reinstallazione Software Gestionali.<br>4. Reinstallazione Software Firewall ed Antivirus.<br>5. RIPRISTINO DATI dall'Hard Disk Esterno o dai CD-ROM.<br>6. Trasferimento dati ripristinati sul Server di Rete.<br>7. Controllo e verifica del ripristino dei dati sull'unità C (Hard Disk Server). |
| **Servizi inerenti all'offerta formativa** | Come sopra | Come sopra |
| **Servizi strumentali agli Organi Collegiali** | Come sopra | Come sopra |

.

UTILIZZO E RIUTILIZZO DEI SUPPORTI MAGNETICI

**I supporti di memorizzazione** di dati sensibili eventualmente utilizzati (hard disk, floppy disk, CD-ROM, chiavi USB, ecc.) sono soggetti alle seguenti misure di sicurezza:

· I floppy disk ed i CD-ROM non più utilizzati devono essere distrutti fisicamente mediante rottura delle parti principali e taglio delle superfici magnetiche, alla presenza dell' incaricato del trattamento;

· Gli Hard Disk non più utilizzabili devono essere distrutti meccanicamente alla presenza dell'Incaricato del trattamento;

· Gli Hard Disk ancora idonei all'uso, come nel caso di sostituzione o dismissione di personal computer, dovranno essere formattati a basso livello alla presenza dell'incaricato del trattamento che dovrà accertare la reale cancellazione di tutti i dati con la collaborazione dell'amministratore di sistema.

## 5.3 MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare, ad ogni variazione, **l'elenco degli incaricati del trattamento dei dati personali.**

In particolare, in caso di trattamento automatizzato di dati, per ogni incaricato del trattamento deve essere indicato lo USER-ID assegnato. In caso di revoca delle autorizzazioni al trattamento dei dati di un Incaricato, il Responsabile del trattamento deve darne immediata comunicazione al Custode delle password e all'amministratore di sistema, che provvederanno a disattivare la possibilità di accesso al sistema per il soggetto in questione. Per redigere l'elenco degli incaricati del trattamento deve essere utilizzato apposito **modulo** , che deve essere conservato a cura del Responsabile del Trattamento dei dati in luogo sicuro.

DEFINIZIONE DEI PERMESSI DI ACCESSO AI DATI

Al Responsabile del trattamento dei dati è affidato il compito di redigere e di aggiornare, ad ogni variazione, **la tabella dei permessi di accesso ad ogni banca di dati** da parte dei soggetti che rivestono la qualità di incaricati del trattamento.

In particolare per ogni incaricato del trattamento e per ogni banca di dati debbono essere indicati i permessi e le autorizzazioni assegnate, tra le quali si riscontrano le seguenti:

- Inserimento di dati.
- Lettura e stampa di dati.
- Variazione o integrazione di dati.
- Cancellazione di dati.

La tabella dei permessi di accesso deve essere redatta utilizzando l'apposito **modulo** che deve essere conservato a cura del Responsabile del trattamento in luogo sicuro e deve essere trasmesso in copia ai seguenti soggetti:

· Amministratore di Sistema.
· Custode delle password.

## 5.4 MANUTENZIONE DELLE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI

MANUTENZIONE DEI SISTEMI DI ELABORAZIONE DEI DATI

All'Amministratore di Sistema è affidato il compito di verificare, ogni anno, la situazione delle apparecchiature hardware installate con cui vengono trattati i dati, delle apparecchiature periferiche ed in particolare dei dispositivi di collegamento con le reti pubbliche. La verifica ha lo scopo di **controllare l'affidabilità e l'efficienza operativa del sistema di elaborazione dei dati**, per quanto riguarda i seguenti profili di rilevanza:

- **Sicurezza dei dati.**
- **Rischio di cancellazione, distruzione o di perdita dei dati.**
- **Rischio di accesso non autorizzato o non consentito** (tenendo conto anche dell'evoluzione tecnologica).

L'Amministratore di Sistema deve compilare apposito **modulo di "Evidenziazione dei rischi Hardware".**
.Nel caso in cui esistano rischi evidenti, il Responsabile del trattamento dei dati deve informarne il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme di legge in vigore.

MANUTENZIONE DEI SISTEMI OPERATIVI

All'Amministratore di Sistema è affidato il compito di verificare ogni anno la situazione dei **Sistemi Operativi** installati sulle apparecchiature con le quali vengono trattati i dati.
La verifica ha lo scopo di controllare l'affidabilità dei Sistemi Operativi, per quanto riguarda i seguenti profili:

- **Sicurezza dei dati.**
- **Rischio di cancellazione, distruzione o di perdita dei dati.**
- **Rischio di accesso non autorizzato o non consentito,** tenendo conto dei seguenti elementi di variazione:

· disponibilità di nuove versioni migliorative dei Sistemi Operativi utilizzati;
· segnalazioni di Patch, Fix o System-Pack per la rimozione di errori o malfunzionamenti;
· segnalazioni di Patch, Fix o System-Pack per l'introduzione di maggiori sicurezze contro i rischi di intrusione o di danneggiamento dei dati.

L'Amministratore di Sistema deve compilare apposito **modulo di "Evidenziazione dei rischi ai Sistemi Operativi**".
Nel caso in cui esistano rischi evidenti, il Responsabile del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme di legge in vigore.

MANUTENZIONE DELLE APPLICAZIONI SOFTWARE

All'Amministratore di Sistema è affidato il compito di verificare ogni anno la situazione delle applicazioni installate sulle apparecchiature con cui vengono trattati i dati.
Anche in questo caso, la verifica ha lo scopo di controllare l'affidabilità del software applicativo per quanto riguarda i seguenti aspetti tecnico-gestionali:

- **Sicurezza dei dati.**
- **Rischio di cancellazione, distruzione o di perdita dei dati.**
- **Rischio di accesso non autorizzato o non consentito.**

Tenendo conto, in particolare, della disponibilità di nuove versioni migliorative delle applicazioni installate che consentano maggiore sicurezza contro i rischi di intrusione o di danneggiamento dei dati, l'Amministratore di Sistema deve compilare apposito **modulo di "Evidenziazione dei rischi nelle Applicazioni Software"**.
Nel caso in cui esistano rischi evidenti, il Responsabile del trattamento dei dati deve informare il Titolare del trattamento perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme di legge in vigore.

## 5.5 MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI

Per ogni archivio di dati trattati con **strumenti non automatizzati**, il Responsabile del trattamento deve definire l'elenco degli incaricati autorizzati ad accedervi , ed impartire istruzioni tese a garantire un controllo costante sull'accesso ad essi. Gli incaricati che trattano atti e documenti contenenti dati personali sono tenuti a conservarli e restituirli al termine delle relative operazioni.
Con riferimento ai documenti contenenti "***dati sensibili e giudiziari "***, gli incaricati sono tenuti a conservarli, fino alla restituzione, in appositi contenitori da riporre in armadi muniti di serratura a chiave. L'accesso agli archivi contenenti documenti ove sono presenti dati sensibili o giudiziari è consentito **previa identificazione e registrazione dei soggetti**, ma non è consentito dopo l'orario di chiusura degli Uffici di Segreteria.

Ai sensi *dell'art. 22, comma 6, del D.Lgs. n. 196/2003*, i dati sensibili e giudiziari contenuti in elenchi, registri o banche dati, sono trattati con **tecniche di cifratura o mediante l'utilizzazione di codici identificativi** o di altre soluzioni che li rendano temporaneamente intelligibili anche a chi è autorizzato ad accedervi, permettendo di identificare gli interessati solo in caso di necessità.
A scopo di sintesi e per completezza espositiva si riporta, nella tabella che segue, l'elenco riepilogativo di tutte le "*misure minime di sicurezza*" adottate o da adottare a cura dell'istituto scolastico:

ELENCO RIEPILOGATIVO DELLE MISURE DI SICUREZZA ADOTTATE

| Tipologia delle misure adottate | Descrizione misura |
|---|---|
| **Fisiche** | Custodia di dati o copie in armadi blindati |
| | Vigilanza sugli accessi negli uffici di segreteria e presidenza |
| | Controllo degli accessi nell'archivio di segreteria |
| | Utilizzo di contenitori con serratura per trasporto documenti contenenti dati sensibili |
| | Utilizzo di classificatori ed armadi blindati |
| | Presenza di dispositivi antintrusione, antifurto ed antincendio |
| | |
| **Logiche** | Nomina del responsabile del trattamento dei dati personali |
| | Nomina degli incaricati del trattamento ed indicazione dei compiti |
| | Nomina dell'amministratore di sistema ed indicazione dei compiti |
| | Nomina del custode delle password ed indicazione dei compiti |
| | Predisposizione delle password e USER ID |
| | Installazione software "firewall" ed antivirus |
| | Controllo degli accessi in rete su ogni singolo client |
| | |
| **Organizzative** | Divulgazione del DPS a tutti gli operatori scolastici |
| | Prescrizione delle linee guida sulla sicurezza a tutti gli incaricati |
| | Formazione del personale scolastico in materia di privacy |
| | Istituzione di un piano di verifica e controllo delle misure adottate |
| | Distruzione dei supporti di memoria da non riutilizzare |

### 5.6 GESTIONE DEGLI STATI DI CRISI E RISPOSTA

Per **gestione degli stati di crisi** si intende il coordinamento complessivo della risposta organizzativa ad una possibile crisi in modo efficace e tempestivo, con lo scopo di evitare o minimizzare i danni alla reputazione ed alla capacità di operare dell'amministrazione scolastica. In caso di incidente devono essere considerate le seguenti priorità:

1) **adottare le misure idonee ad evitare danni diretti alle persone;**
2) **proteggere adeguatamente l'informazione o il dato personale, sensibile o giudiziario messo in pericolo;**
3) **evitare o limitare i danni economici;**
4) **limitare i danni all'immagine dell'Amministrazione Scolastica.**

Garantita l'incolumità fisica alle persone, le situazioni di crisi devono immediatamente essere comunicate all'Amministratore di Sistema ed al Responsabile del trattamento che provvederanno a porre in essere le seguenti cautele:

- isolare e delimitare l'area contenente il sistema oggetto dell'incidente ;
- isolare il punto del sistema compromesso dalla rete nel suo complesso;
- spegnere correttamente il sistema ;
- provare a ripristinare il sistema secondo le procedure tecniche previste;
- effettuare Test di operatività;
- ripristinare e far riprendere l'operatività normale;
- documentare tutte le operazioni compilando un report da consegnare al Titolare del trattamento.

PIANO DI VERIFICA DELLE MISURE ADOTTATE

**L'efficienza e l'operatività delle misure adottate deve essere periodicamente verificata**.
In particolare occorre:

- Verificare l'acceso fisico ai locali ove si svolge il trattamento (a cura del Responsabile, ogni 2 mesi);
- Verificare il corretto utilizzo delle parole chiave e dei profili di accesso degli incaricati, prevedere la disattivazione dei codici di accesso decaduti per più di 3 mesi (a cura dell'Amministratore, ogni 3 mesi);
- Verificare l'integrità dei dati e delle loro copie di backup (a cura del Responsabile, ogni mese);
- Verificare che i sistemi informatici siano regolarmente aggiornati in termini di patch ed antivirus (a cura dell'Amministratore, ogni 2 mesi);
- Verificare la bontà di conservazione dei documenti cartacei (a cura del Responsabile, ogni 6mesi);

· Verificare la distruzione dei supporti magnetici che non possono più essere riutilizzati (a cura del Responsabile, ogni mese);

· Verificare il livello di formazione degli incaricati, prevedere sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica (a cura del Responsabile con cadenza annuale).

## 6. PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

### 6.1 PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO Al TRATTAMENTO DEI DATI

Il presente piano è soggetto a **revisione annua obbligatoria con scadenza entro il 31 marzo**, ai sensi dell'art. 19 allegato B del D.Lgs. 196/2003. Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- **modifiche all'assetto organizzativo della Scuola** ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- **danneggiamento o attacchi al patrimonio informativo della Scuola** tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

Al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 31 agosto, le necessità di formazione del personale incaricato del trattamento dei dati, con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza nel trattamento dei dati.
Per ogni incaricato del trattamento, il Responsabile del trattamento definisce, sulla base dell'esperienza e delle sue conoscenze ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata, utilizzando apposito modulo che deve essere trasmesso al Titolare del trattamento.
In ogni caso la **formazione degli incaricati** dovrà prevedere sicuramente le **seguenti materie**:

• Una analisi dettagliata ed aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee in materia di trattamento dei dati e tutela della riservatezza;
• Lettura e analisi dei principi sanciti dalla **Costituzione Italiana** in materia di diritti fondamentali della persona;
• Disposizioni legislative in tema di tutela dei dati personali e studio della **criminalità informatica**;
• Analisi dettagliata del *D.Lgs. n. 196/2003* e della normativa collegata;
• Analisi del nuovo ***Regolamento sul trattamento dei dati sensibili e giudiziari*** (D.M. n. 305/2006);
• Analisi e studio dei **ruoli soggettivi** di Titolare, Responsabile, Incaricato, Amministratore di Sistema, Custode delle password, soggetti interessati al trattamento dei dati;
• Panoramica sugli adempimenti ex D.Lgs. n. 196/2003: notificazione, rapporti con gli interessati, rapporti con il l'Ufficio del Garante della Privacy.
• **Misure minime di sicurezza** con particolare riferimento ai seguenti argomenti: criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software, sistemi di allarme antintrusione, importanza e modalità di realizzazione delle operazioni di backup e salvataggio.

La formazione del personale costituisce elemento fondamentale per la garanzia di un efficiente ed efficace funzionamento di ogni struttura organizzativa e rappresenta supporto indispensabile per l'effettiva implementazione delle disposizioni previste dal *D.L.vo 196/2003.*

### 6.2 PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI

| ***Descrizione dell'intervento*** | ***Struttura interessata*** | ***Destinatari*** | ***Periodo*** |
|---|---|---|---|
| Illustrazione aggiornamenti *D.P.S.* anno 2011 | - Dirigente scolastico<br>- DSGA | Personale Docente ed ATA | Date da programmare (periodo Aprile – Giugno 2011) |
| Presentazione ed illustrazione del nuovo "*Regolamento sul trattamento dei dati sensibili e giudiziari"*.<br>Relazione del DS e DSGA.<br>Distribuzione di opuscoli e fogli informativi al personale dipendente. | - Dirigente scolastico<br>- DSGA | Personale Docente ed ATA | Date da programmare (periodo Settembre – Ottobre 2011). |
| Utilizzo delle tecnologie informatiche e rischi connessi all'utilizzo della Rete Internet.<br>L'adozione delle *misure minime di sicurezza* nel trattamento dei dati. | - Dirigente Scolastico<br>- DSGA<br>- Amministratore di Sistema | Personale ATA | Date da programmare (periodo Novembre – Dicembre 2011). |

## 7. TRATTAMENTI DI DATI PERSONALI AFFIDATI A SOGGETTI ESTERNI

L'affidamento del trattamento di dati dell'istituto a soggetti esterni è subordinato ad una espressa previsione di legge . Nel caso di affidamento, da parte della istituzione scolastica, a **soggetti esterni** di attività che comportino trattamento di dati personali, occorre distinguere due casi:

a) **affidamento a persone fisiche;**
b) **affidamento a persone giuridiche;**

### 7.1 AFFIDAMENTO A PERSONE FISICHE

Nel caso in cui il soggetto affidatario sia una persona fisica, lo stesso sarà designato dal Titolare o dal Responsabile mediante atto di nomina individuale che specifichi puntualmente le regole di comportamento da osservare.
Ove necessario, il Titolare o il Responsabile provvederanno a informare l'incaricato sui contenuti fondamentali delle norme che disciplinano il trattamento dei dati personali agli effetti del vigente *Codice* (D.Lgs.196/2003).
Il Titolare o il Responsabile verificheranno periodicamente, nelle forme ritenute più opportune, la correttezza del trattamento, con particolare riferimento all'adozione delle **misure minime di sicurezza** da parte degli incaricati.

### 7.2 AFFIDAMENTO A PERSONE GIURIDICHE

Nel caso che il soggetto affidatario sia una persona giuridica, la stessa sarà designata dal Titolare o dal Responsabile mediante un atto di nomina che specifichi puntualmente le norme di comportamento da seguire, con specifico riferimento alle **misure minime di sicurezza** da adottare.
Il Titolare vigilerà sulle attività relative al trattamento e si farà rilasciare dallo stesso una dichiarazione di conformità a quanto stabilito dalle norme di legge e dal presente Documento.
Il Titolare del trattamento può decidere di affidare il trattamento dei dati, in tutto o in parte, a soggetti terzi, nominandoli responsabili del trattamento. In questo caso debbono essere specificati i soggetti interessati e i luoghi dove fisicamente avviene il trattamento dei dati stessi.. Il Titolare del trattamento deve informare il Responsabile del trattamento dei dati dei compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore, ed in particolare di quanto stabilito dal D. Lgs. n. 196/2003.
Il Responsabile del trattamento dei dati deve rilasciare una dichiarazione scritta al Titolare del trattamento da cui risulti che sono state adottate le misure idonee di sicurezza per il trattamento dei dati secondo quanto disposto dal D.L.gs. n. 196/2003.
La nomina del Responsabile del trattamento dei dati deve essere controfirmata per accettazione e copia della lettera di nomina accettata deve essere conservata a cura del Titolare del trattamento in luogo sicuro.

VINCOLI CONTRATTUALMENTE ASSUNTI DAL SOGGETTO ESTERNO
AI FINI DELLA SICUREZZA DEI DATI

Qualora l'Istituzione Scolastica dovesse procedere, nei casi consentiti dalla legge, ad **affidare all'esterno il trattamento di alcuni dati personali**, tale trattamento dovrà avvenire previa assunzione da parte dell'affidatario – nell'ambito dello stesso contratto con cui viene realizzato l'affidamento o con atto aggiuntivo – degli **impegni derivanti dalle seguenti dichiarazioni**:
**1.** di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali, sono soggetti all'applicazione del D.Lgs. n. 196/2003;
**2.** di adottare le istruzioni specifiche ricevute per il trattamento dei dati personali e di integrarle nelle procedure già in essere;
**3.** di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di avvertire immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
**4.** di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

CONSULENTI ESTERNI, COLLABORATORI E SPECIALISTI

Nel caso in cui l'Istituzione Scolastica dovesse avvalersi, per **l'attuazione di interventi previsti dall'offerta formativa o dagli interventi miranti all'integrazione dei soggetti diversamente abili**, della collaborazione di terapisti, esperti esterni, specialisti o assistenti medico-sanitari, è escluso, nei limiti del possibile, l'accesso dei medesimi a documentazioni contenenti "*dati sensibili*". In merito alla possibilità di trattamento di ulteriori dati sensibili da parte dei suddetti soggetti, è previsto che i medesimi dichiarino:

1. di essere consapevoli degli obblighi previsti dal *D. Lgs n. 196/2003;*
2. di impegnarsi ad ottemperare all'obbligo di tutela dei dati personali;
3. di adottare le istruzioni specifiche ricevute per la garanzia di sicurezza dei dati.

Si applicano, in ogni caso, le previsioni contenute nel *Regolamento sul trattamento dei dati sensibili e giudiziari* (D.M. n. 305/2006), a garanzia della tutela del diritto alla riservatezza degli interessati.

PUBBLICAZIONE DOCUMENTI SUL SITO WEB DELL'ISTITUTO

Il sito web dell'Istituto è registrato all'indirizzo **http://www.istitutoleonori.it** ed è aggiornato dal Dirigente Scolastico, al quale è demandata la supervisione ed il coordinamento delle attività di gestione del sito svolte dai docenti interessati.

**REQUISITI PER LA PUBBLICAZIONE DEI MATERIALI SUL SITO WEB:**

Poiché il materiale pubblicato esprime i contenuti dell'offerta formativa della Scuola e concorre, pertanto, a determinare l'immagine dell'istituzione all'esterno, è necessario curare costantemente le caratteristiche dei prodotti da mettere in rete, sotto il profilo della loro rispondenza agli **standard formativi ed educativi** dell'Istituto.

- **Pubblicazione di immagini e foto**

Qualora debbano essere pubblicate foto nelle quali siano riconoscibili gli alunni, i docenti coordinatori delle classi interessate dovranno acquisire preventivamente **un'autorizzazione dei genitori alla pubblicazione dell'immagine (liberatoria)**, utilizzando un apposito modulo fornito dall'Ufficio di Segreteria. Per gli alunni privi di autorizzazione si provvederà a sfumare il volto in modo da renderli non riconoscibili. Non è necessaria l'autorizzazione per l'inserimento di immagini fotografiche di adulti, qualora siano ritratti in un contesto normale privo di profili di riservatezza.

- **Divieto di pubblicazioni illecite**

E' vietato pubblicare sul sito web informazioni, documenti ed ogni altro materiale avente contenuto **diffamatorio, osceno, riservato** o di cui non è consentita la distribuzione in via telematica. Non è possibile, altresì, pubblicare materiale con **scopi contrari all'ordine pubblico ed alla sicurezza dello Stato,** o con scopi contrari alla morale ed al buon costume.

- **Tutela del diritto d'autore**

Non possono essere pubblicati articoli o materiali coperti dal **diritto d'autore**, nelle due forme del diritto morale d'autore (diritto alla paternità dell'opera dell'ingegno) e del diritto patrimoniale d'autore (diritto allo sfruttamento economico dell'opera).

- La riproduzione, la pubblicazione e la distribuzione, totale o parziale, di tutto il materiale contenuto all'interno del sito sono espressamente vietati in assenza di una autorizzazione scritta da parte del Dirigente Scolastico.

**NORMATIVA CHE REGOLA L'UTILIZZO DELLE RETI TELEMATICHE**

Si richiama la normativa vigente che regola l'utilizzo delle reti telematiche:

- D. Lgs. 30/06/2003 n° 196 (Codice Privacy).
- D.P.R. 10/11/1997 n° 513 (Regolamento contenente i criteri e le modalità per la formazione, l'archiviazione e la trasmissione di documenti con strumenti informatici e telematici , a norma dell'art.15,comma 2, della Legge 15/03/1997 n° 59).
- Legge 22/04/1941 n° 633 in materia di tutela del diritto d'autore (testo coordinato e integrato con le ultime modifiche introdotte dalla Legge 18/08/2000 n° 248.
- D. Lgs. 29/12/1992 n° 518 (attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratori).

## 8. DICHIARAZIONE DI IMPEGNO

Il **Dirigente Scolastico**, in qualità di Titolare del trattamento dei dati, **si impegna ad adottare**, nella fase di graduale attuazione degli interventi previsti dalla normativa sulla tutela della *privacy,* ogni possibile **misura idonea a salvaguardare la sicurezza dei dati personali**, siano essi contenuti nei documenti cartacei che trattati e registrati mediante strumenti elettronici. Tali misure riguarderanno gli aspetti organizzativi, logistici e procedurali miranti ad evitare con ogni mezzo qualsiasi incremento di rischi di distruzione o perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito.

## 9. OBBLIGO DI AGGIORNAMENTO DEL DPS E SUE REVISIONI

Il presente ***Documento Programmatico sulla Sicurezza*** è sottoposto a **revisione annuale** nella sua interezza entro la scadenza del 31 Marzo di ogni anno, come previsto dalla regola n. 19 del Disciplinare tecnico di cui all'allegato B) al *D.Lgs. n. 196/2003*, in relazione al disposto dell'art. 34, lettera g) del decreto stesso.

Per quanto non espressamente previsto e regolato nel presente Documento, si applicano in via sostitutiva le norme generali contenute nel D.Lgs. n. 196/2003 (e successive modifiche ed integrazioni).

Data dell'ultimo aggiornamento: 10/03/2011.

Al presente documento è stata attribuita **data certa** mediante formale adozione con decreto del Dirigente Scolastico (Decreto registrato al progressivo n. 2570 del 10/03/2011).

**Il Responsabile del trattamento**
DIRETTORE S.G.A.
*(C. Roberto Dieli)*

**Il Titolare del trattamento**
DIRIGENTE SCOLASTICO
*(Dott.ssa Lina Porrello)*