



**ISTITUTO COMPRENSIVO
UMBERTO I
PITIGLIANO**

**DOCUMENTO PROGRAMMATICO
SULLA SICUREZZA DEI DATI**

(ai sensi del D.lvo 196/2003)

(REVISIONE N.. 05 - 2011)

Prot: 1046 a35 del 09/03/2011

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI PERSONALI **(D. L.vo 196 del 30/06/03)**

PREMESSA

L'Istituto Comprensivo Statale "Umberto I" con sede in Pitigliano - Piazza Dante Alighieri, 19 C.F. 82002750535, nella persona del suo legale rappresentante Dirigente Scolastico Prof.ssa Daniela Busoni ha redatto il seguente Documento Programmatico per la Sicurezza ai sensi e per gli effetti dell'art. 34 comma 1, lettera g) del D. L.vo n. 196/2003 e del disciplinare tecnico allegato al medesimo sub B "Disciplinare tecnico in materia di misure minime di sicurezza", nonché della "Guida operativa per redigere il documento programmatico" pubblicata sul sito web del Garante.

Scopo del presente documento, di seguito denominato "DPS" è quello di delineare il quadro delle misure di sicurezza, organizzative, fisiche e logistiche, secondo la descrizione e gli opportuni allegati, che fanno parte integrante del Documento, che saranno adottate da questa Istituzione Scolastica relativamente al trattamento dei dati personali, per le rispettive competenze, da parte del DSGA, degli Assistenti Amministrativi, del Personale Docente e dei Collaboratori Scolastici.

ARTICOLO 1 **RIFERIMENTI NORMATIVI**

- Legge 31/12/1996 n. 675 e successive modifiche;
- Legge 31/12/1996 n. 676, recante delega al governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- DPR 28/07/1999, n. 318 - Regolamento recante norme per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali;
- Legge 24/03/2001 n. 127, recante delega al governo per l'emanazione di un T. U. in materia di trattamento dei dati personali;
- Decreto legislativo 30/06/2003 n. 196 - Codice in materia di protezione dei dati personali, in particolare:
 - degli articoli 20, comma 2, e 21, comma 2, (identificazione e natura dei dati trattati)
 - degli articoli da 28 a 30 (Soggetti che effettuano il trattamento);
 - degli articoli dal 31 al 36 (misure di sicurezza);
 - degli articoli 59 e 60 (Disposizioni relative a specifici settori - Trattamento in ambito pubblico);
 - degli articoli 95 e 96 (Disposizioni relative a specifici settori - Istruzione);
 - dell'articolo 180 (Disposizioni transitorie - Misure di sicurezza);
 - dell'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza);
- del Decreto 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 dei citati articoli 20 e 21 del D.Lgs. 196/03)

Per "definizioni" si rispettano quelle riportate all'art. 4 del D.L.vo 196/2003;

- Linee Guida del Garante per posta elettronica e internet (G.U. n.58 del 10 marzo 2007)
- Provvedimento del Garante per la protezione dei dati personali del 13.10.08 " Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali"
- Provvedimento del Garante per la protezione dei dati personali del 27.11.08 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema"

ARTICOLO 2 **OBIETTIVI DEL DOCUMENTO**

Il "DPS", redatto in ottemperanza a quanto disposto dal D.L.vo 196/2003 (Codice in materia di protezione dei dati personali) mira a regolamentare e garantire la riservatezza, la sicurezza e la Protezione dei dati personali in possesso dell'Istituto Comprensivo "Umberto I", nonché a porre in atto idonee strategie per la protezione delle aree e dei locali interessati a misure di sicurezza.

Il Documento garantisce che il trattamento dei dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Il tutto è disciplinato in modo da assicurare un elevato livello di tutela dei diritti e delle libertà, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte del titolare del trattamento (art. 2 D.L.vo 196/2003). Ai sensi dell'art.1 del D.L.vo: "Chiunque ha diritto alla protezione dei dati personali che lo riguardano". Tali dati sono quelli sensibili e non previsti a seguito dei trattamenti indicati dal Decreto 7 dicembre 2006, n. 305 e in parte di seguito riepilogati:

- del personale che presta servizio presso l'istruzione scolastica;
- degli alunni che frequentano questa Scuola;
- dei genitori degli alunni o gli esercenti la potestà familiare per le notizie che trasmettono o portano a scuola;
- dei fornitori.

In particolare, nel "DPS" vengono definiti i criteri tecnici e organizzativi per:

- a) la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ad accedere ai medesimi locali;
- b) i criteri e le procedure per assicurare l'integrità dei dati;
- c) i criteri e le procedure per la sicurezza della trasmissione dei dati, cartacei o telematici;
- d) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati e dei modi per prevenire gli eventi dannosi.

ARTICOLO 3 **ELENCO DEI TRATTAMENTI DEI DATI PERSONALI**

Dati trattati dai docenti

Le banche dati cui ha accesso il singolo docente sono:

- Il registro personale
- Gli elaborati

Le banche dati cui hanno accesso più docenti sono:

- Il registro di classe
- Il registro dei verbali del consiglio di classe
- La documentazione relativa alla programmazione didattica
- I documenti di valutazione
- La documentazione dello stato di handicap
- La corrispondenza con le famiglie

- La documentazione giustificativa delle assenze degli alunni (es. festività religiose, certificati medici, etc.)

I dati trattati dai docenti per l'attività educativa, didattica, formativa e di valutazione sono nel loro insieme dati sensibili, ai sensi dell'art. 4 del D.Lvo n. 196 del 30 giugno 2003 comma 1 lett. b,c,d e come specificato nella scheda n. 5 del Decreto 7 dicembre 2006, n. 305. Il trattamento dei dati da parte dei docenti (tenuta dei registri, modalità di compilazione dei documenti di valutazione, verbalizzazione, etc.) è definito puntualmente da norme di legge o regolamentari.

Dati trattati dal personale amministrativo

Le banche dati su supporto cartaceo e/o informatizzato, contenenti dati personali, cui ha accesso il personale di segreteria, raggruppati in insiemi omogenei, sono:

- i fascicoli relativi al personale della scuola
- i fascicoli alunni e ex alunni
- l'anagrafe fornitori
- i contratti e convenzioni
- documentazione finanziaria e contabile
- la documentazione didattica trattata dal docenti per la conservazione
- il registro degli infortuni
- gestione del contenzioso

Dati trattati dal dirigente scolastico

Le banche dati di pertinenza del dirigente sono:

- fascicoli del personale Direttivo, Docente e Amministrativo
- i verbali delle assemblee degli Organi Collegiali
- la programmazione relativa allo stato di disagio (handicap)
- il protocollo riservato
- il fascicolo del personale in prova
- gestione del contenzioso e dei provvedimenti disciplinari

ARTICOLO 4 **CAMPO DI APPLICAZIONE**

- 1.** Il "DPS" definisce le politiche e gli standard di sicurezza in merito ai dati da garantire e proteggere. Tali dati si distinguono in:
 - **dati personali comuni** (dati anagrafici o identificativi delle persone, indirizzi recapiti telefonici, codici fiscali, dati bancari, informazioni circa la composizione familiare, la professione esercitata da un determinato soggetto, la sua formazione etc.);
 - **dati sensibili** (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, appartenenza a categorie protette, portatore di handicap, stato di gravidanza , vita sessuale etc.);
 - **dati giudiziari** (provvedimenti sul casellario giudiziale, anagrafe delle sanzioni amministrative dipendenti da reato o dei relativi carichi pendenti, la qualità di imputato indagato ai sensi degli artt. 60 o 61 del Codice di Procedura Penale, avviso di garanzia o m la, separazioni, affidamento dei figli, etc.).
- 2.** I trattamenti sono realizzati prevalentemente negli uffici di presidenza e segreteria, nell'archivio della sede centrale, nelle aule scolastiche ove sono conservati, durante l'anno scolastico, i registri di classe, il giornale dell'insegnante, i documenti di valutazione degli alunni .
- 3.** I dati sono trattati con fascicoli e atti cartacei e con strumenti elettronici di elaborazione
- 4.** Il Responsabile e gli Incaricati di effettuare il trattamento dei dati utilizzano i fascicoli cartacei e i personal computer in dotazione degli uffici.
- 5.** I computer degli uffici di segreteria sono collegati in rete e ad internet.

6. Gli Incaricati che hanno accesso ad atti e documenti informatici degli uffici sono forniti di password personali. Tali password sono adeguatamente custodite in buste chiuse dal Responsabile in luogo sicuro.

ARTICOLO 5

SOGGETTI CHE EFFETTUANO IL TRATTAMENTO PER LA PROTEZIONE DEI DATI PERSONALI

Il D.L.vo 196/2003 sulla protezione dei dati personali individua all'art. 4 i soggetti che sono coinvolti nel trattamento dei dati personali:

- **il titolare:** la persona fisica e giuridica cui compete la responsabilità finale ed assume decisioni fondamentali riferite alle modalità di trattamento dei dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;
- **il responsabile:** la persona fisica, dotata di particolari caratteristiche di natura morale e di competenza tecnica, con precise capacità ed affidabilità, preposta dal titolare al trattamento dei dati personali;
- **gli incaricati:** le persone fisiche autorizzate a compiere operazioni di trattamento e che materialmente provvedo al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile;
- **l'amministratore di sistema:** il soggetto cui è conferito il compito di "sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base di dati e di consentirne l'utilizzazione". Tale figura è individuata dall' art. 1 del DPR 318/99, mentre non viene riproposta nel D.L.vo 196/2003 che pur conserva una propria funzionalità per la garanzia delle misure di sicurezza logica del sistema informatica della gestione dei dati. Pertanto si ravvisa la necessità di individuare tale figura con delega di compiti definiti.

1. IL TITOLARE DEL TRATTAMENTO (art. 28 D.L.vo 196/2003)

Titolare del trattamento, come definito nella Premessa, è il legale rappresentante pro tempore di questa Istituzione Scolastica, Dirigente Scolastico prof.ssa **Daniela Busoni**.

E' onere del Titolare del trattamento individuare, nominare e incaricare per iscritto uno o più Responsabili del trattamento dei dati, che assicurano e garantiscano che vengano adottate le misure di sicurezza.

Il Titolare del trattamento affida al Responsabile del trattamento dei dati il compito di adottare le misure tese a ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita dei dati medesimi, anche accidentale, l'accesso non autorizzato o il trattamento non consentito, previe istruzioni fornite per iscritto (art. 31 D.L.vo 196/2003).

2. RESPONSABILE DEL TRATTAMENTO (art. 29 D.L.vo 196/2003)

In relazione all'attività del Titolare del trattamento, è prevista la nomina di uno o più Responsabili del trattamento, con compiti diversi a seconda delle funzioni svolte.

Il Responsabile è individuato tra soggetti che per esperienza , capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

I compiti affidati al Responsabile sono analiticamente specificati per iscritto dal Titolare (art. 29 c. 4 D. L.vo 196/03). Il Titolare del trattamento affida al Responsabile del trattamento l'onere di individuare, nominare ed indicare per iscritto gli Incaricati del trattamento.

In particolare, il Titolare del trattamento, designa e nomina quale Responsabile del trattamento dei dati:

il D.S.G.A. di questa Istituzione Scolastica, Sig. **Daniele Rappoli** per la parte amministrativa ed economica, e per il personale non docente in quanto persona con capacità professionali, esperienza e affidabilità, tale da fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento dei dati. **(REVISIONE N. 03 DEL 20/09/2010).**

Il Responsabile del trattamento dei dati ha il compito di:

- Attribuire ad ogni utente (User) o Incaricato un codice identificativo personale (User-id) per l'autorizzazione dell'elaboratore;
- Verificare con cadenza almeno quindicinale, l'efficacia dei programmi di protezione ed antivirus, nonché delle le modalità di accesso ai locali;
- Informare il Titolare nella eventualità che si siano rilevati dei rischi.

Altresì al Responsabile del trattamento dei dati è affidato il compito di **gestire e custodire le password** per l'accesso ai dati da parte degli Incaricati. Egli predispone, per ogni Incaricato del trattamento, una busta sulla quale è indicato lo USER-ID utilizzato: all'interno della busta deve essere indicata la password utilizzata dall'Incaricato per accedere alla banca-dati.

Le buste con le password debbono essere conservate in luogo chiuso e protetto.

Il Titolare del trattamento dei dati informa il Responsabile sui compiti che gli sono affidati in relazione a quanto disposto dalle normative in vigore fornendogli una copia di tutte le norme che riguardano la sicurezza del trattamento dei dati in vigore al momento della nomina.

La nomina del Responsabile del trattamento è annuale e può decadere per revoca in qualsiasi momento o con il venir meno dei compiti che giustificavano il trattamento.

3. GLI INCARICATI DEL TRATTAMENTO (art. 30 D.L.vo 196/2003)

Al Responsabile del trattamento è affidato il compito di nominare, con comunicazione scritta, gli Incaricati del trattamento dei dati.

La designazione di ciascun Incaricato del trattamento dei dati viene effettuata con lettera di incarico in cui sono ben specificati i compiti che gli sono affidati e l'ambito del trattamento consentito come indicato anche nel regolamento per il trattamento dei dati sensibili e giudiziari.

Gli Incaricati del trattamento potranno se necessario ricevere idonee ed analitiche istruzioni scritte, anche per gruppi omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti.

La nomina degli Incaricati del trattamento deve essere controfirmata dall'interessato per presa visione.

In particolare, tenuto conto del piano di lavoro e delle attività predisposto dal DSGA per il corrente anno scolastico e adottato dal D.S., **il Responsabile del trattamento individua e nomina i seguenti Incaricati con annesso ambito del trattamento dei dati consentito:**

Gli incaricati al trattamento dati saranno:

TUTTI GLI ASSISTENTI AMMINISTRATIVI

nei loro specifici incarichi o nelle loro mansioni generali previste dal CCNL nell'area specifica di appartenenza (attività lavorativa complessa con autonomia operativa e responsabilità diretta nella definizione e nell'esecuzione degli atti a carattere amministrativo e contabile di ragioneria e di economato, pure mediante l'utilizzazione di procedure informatiche; gestione dei fascicoli personali del personale e degli alunni; rilevazione e gestione delle assenze, compilazione delle certificazioni relative al personale e agli alunni; accoglienza del pubblico) osserveranno la massima privacy, evitando di diffondere notizie che devono restare private.

Tale personale deve ricevere idonee ed analitiche informazioni da parte del Responsabile del trattamento sulle mansioni loro affidate e sugli adempimenti cui sono tenuti in ragione della riservatezza che si deve per l'incarico affidato e per il fatto di essere dipendenti di questa pubblica istituzione scolastica.

Agli Incaricati del trattamento il Responsabile consegnerà una copia della normativa che riguarda la sicurezza del trattamento dei dati in vigore al momento della nomina. Tale nomina è per anno scolastico e può decadere per revoca, o con il venir meno dei compiti che giustificavano il trattamento.

TUTTI I COLLABORATORI SCOLASTICI

Nei loro specifici incarichi o nelle loro mansioni generali previste dal CCNL nell'area specifica di appartenenza (accoglienza e sorveglianza nei confronti degli alunni, ausilio materiale nei confronti degli alunni in situazione di difficoltà, custodia e sorveglianza nei locali scolastici, vigilanza nei confronti del pubblico evitando ed impedendo l'intrusione di persone estranee, collaborazione con i docenti e con il personale di segreteria, pulizia dei locali) osserveranno la massima privacy, evitando di diffondere notizie che devono restare private, in particolare quando ricevono o portano in giro Circolari Ministeriali, Note degli Uffici Superiori o circolari interne in visione al personale docente.

Tale personale deve ricevere idonee ed analitiche informazioni da parte del Responsabile del trattamento sulle mansioni loro affidate e sugli adempimenti cui sono tenuti in ragione della riservatezza che si deve per l'incarico affidato e per il fatto di essere dipendenti di questa pubblica istituzione scolastica.

Agli Incaricati del trattamento il Responsabile consegnerà una copia della normativa che riguarda la sicurezza del trattamento dei dati in vigore al momento della nomina. Tale nomina è per anno scolastico e può decadere per revoca, o con il venir meno dei compiti che giustificavano il trattamento.

TUTTI I DOCENTI

Docenti a tempo indeterminato o determinato e tutte le altre unità di personale che a qualunque titolo hanno rapporto di lavoro anche occasionale (stipule di contratti o convenzioni) con l'Istituzione Scolastica eviteranno di diffondere notizie che resteranno segrete sia per quanto attiene i dati personali comuni, sia per i dati sensibili che hanno acquisito in virtù del loro ufficio.

Il docente, per la sfera di competenza, rientra nell'ambito degli incaricati sia per le categorie di dati cui può accedere, sia per la tipologia di trattamento e vincoli specifici ai sensi dell'art. 4 del D.L.vo 196/2003, sia per le istruzioni in merito al soggetti cui i dati possono essere comunicati o diffusi. I dati trattati dai docenti si rinvergono nei registri dei verbali degli OO.CC., nei registri di classe, dell'insegnante, nei documenti di valutazione, nelle diagnosi funzionali per la situazione di handicap, nelle assenze degli alunni, in eventuali certificati medici, etc. Il trattamento dei dati da parte dei docenti è definito puntualmente da norme di legge.

Tale personale riceverà specifica informazione/formazione da parte del Titolare del trattamento e/o dal Responsabile del trattamento circa gli specifici doveri e gli adempimenti cui sono tenuti in ragione del loro ufficio, della riservatezza che si deve ai dati che trattano per il fatto di essere dipendenti di questa pubblica istituzione scolastica.

4. RESPONSABILE DEL SISTEMA INFORMATICO DELL'AMMINISTRAZIONE

Dato l'elevato utilizzo delle strumentazioni informatiche, il Titolare del trattamento ritiene opportuno conferire la nomina di responsabile del sistema informatico dell'amministrazione a persona particolarmente competente individuata nella figura del Responsabile del Trattamento dati. Tale persona è stata individuata in quanto persona capace, idonea nell'utilizzo dei sistemi informatici e dei relativi programmi.

Il responsabile del sistema informatico dell'amministrazione incaricato con atto scritto

- rispetta le misure di sicurezza previste dalla legge e specificate nel DPS;
- garantisce la massima riservatezza nel trattamento dei dati;
- informa tempestivamente il Titolare di anomalie nel funzionamento del sistema informatico che possono pregiudicare il corretto trattamento dei dati.
- prende tutti i provvedimenti necessari ad evitare la perdita o la distruzione dei dati e provvede al ricovero periodico degli stessi con copie di back up;
- si assicura della qualità delle copie di back up dei dati e della loro conservazione in luogo adatto e sicuro (cassaforte del DSGA);

- fa in modo che sia prevista la disattivazione dei Codici identificativi personali (User-Id), in caso di perdita della qualità che consentiva all'utente o incaricato l'accesso all'elaboratore, oppure nel caso di mancato utilizzo dei Codici identificativi personali per oltre 6 mesi;
- protegge gli elaboratori dal rischio di intrusione (violazione del sistema da parte di "hackers") e dal rischio di virus mediante idonei programmi.
- Si precisa che nei laboratori informatici presenti nella sede centrale e nelle sezioni associate non sono conservate banche dati ossia non sono presenti dati di tipo personale e sensibile.

ARTICOLO 6

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

1. Le situazioni dei rischi che incombono sui dati possono riguardare:
 - Dati su materiale cartaceo;
 - Dati su attrezzature informatiche;
 - I luoghi e i contenitori che custodiscono sia i materiali cartacei, sia le attrezzature informatiche.
2. I materiali cartacei a rischio sono:
 - Raccoglitori e faldoni che raccolgono i documenti contenuti nei fascicoli del personale;
 - Schede personali degli alunni;
 - Documenti di valutazione delle competenze;
 - Registri (di classe, dell'insegnante, di presenza);
 - Registro dello stato del personale;
 - Decreti e certificati sulle persone;
 - Anagrafe fornitori;
 - Contratti e convenzioni;
 - Documentazione finanziaria e contabile;
 - Registro infortuni;
 - Moduli di iscrizione, istanze, etc
 - Atti affissi agli albi.
3. I dati informatici a rischio sono quelli contenuti nei documenti di cui al precedente articolo e immessi nel personal computer degli uffici.
4. Gli eventi che possono generare danni e che comportano rischi per la sicurezza dei dati personali si distinguono sotto un triplice aspetto:
 - a) Comportamento degli operatori:
 - Sottrazioni di credenziali di autenticazione;
 - Carenza di consapevolezza, disattenzione o incuria;
 - Manomissioni e comportamenti sleali o fraudolenti;
 - Errore materiale.

In merito all'errore materiale, si considera tale anche la produzione di atti o documenti viziati o errati; qualora il foglio da scartare contenga dei dati sensibili bisogna provvedere alla sua distruzione, per tale ragione si dovrà dotare l'ufficio di un distruggi-documenti a strisce.

b) Eventi relativi agli strumenti:

- Azione di virus informatici o di programmi suscettibili di recare danno;
- Spamming, tecnica di sabotaggio o posta spazzatura: vettore attraverso il quale si fanno circolare virus e codici maligni di ogni tipo con l'obiettivo di compromettere il funzionamento dei computer a catena e rendere al contempo più difficile il tracking, cioè l'individuazione da parte delle forze di polizia preposte al compito di garantire la sicurezza della società dell'informazione, ma è altresì piaga planetaria e veicolo per vendere software contraffatti, in una sorta di e-commerce illegale;
- Hacker: persona che utilizza la sua abilità informatica in modo fraudolento con lo scopo di elaborare un virus o Penetrare in una rete di computer protetta;
- Malfunzionamento, indisponibilità o degrado degli strumenti;
- Accessi esterni non autorizzati;
- Intercettazione di informazioni in rete.

c) Eventi relativi al contesto fisico-ambientale:

- Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, etc.), nonché dolosi, accidentali o dovuti ad incuria;
- Accesso di estranei o persone non titolari di incarichi e responsabilità nel trattamento dei dati
- Errori umani nella gestione della sicurezza fisica.
- Accessi esterni non autorizzati;
- Vandalismo;
- Intercettazioni di informazioni in rete;
- Sottrazione di strumenti contenenti dati;
- Guasto ai sistemi complementari (impianto elettrico, gruppo di continuità, etc.).

ARTICOLO 7**ANALISI DELLA SITUAZIONE ATTUALE DELL'ISTITUZIONE SCOLASTICA**

Per procedere all'analisi dei rischi che incombono sui dati è necessario descrivere ed analizzare la situazione attuale della istituzione scolastica.

7.1 Situazione attuale

I dati che seguono sono relativi a una rilevazione effettuata a febbraio 2010

7.1.1 Plessi e loro collocazione

SEDE PRINCIPALE Presidenza e uffici di segreteria	P.za Dante Alighieri Tel 0564 616035	Pitigliano
SCUOLA PRIMARIA	P.za Dante Alighieri Tel 0564 616035	Pitigliano
SEDE ASSOCIATA SCUOLA INFANZIA	Via Madonna del Fiore 0564/616323	Pitigliano
SEDE ASSOCIATA SCUOLA SECONDARIA DI PRIMO GRADO	Via Don Minzoni 0564/616308	Pitigliano

7.1.2 Locali dove avviene il trattamento dei dati effettuato da personale docente

I locali ove avviene il trattamento dei dati effettuato da docenti coincidono con quelli adibiti ad attività didattica, allocati nei plessi costituenti l'istituzione scolastica. Nelle scuole in questione sono presenti alcuni arredi, armadi in legno e metallo, in generale non idonei a contenere i dati personali secondo le prescrizioni di legge, in alcune cattedre dei docenti sono presenti cassette con chiusure senza chiave. Esistono nei plessi locali di pertinenza esclusiva dei docenti (sale insegnanti) .

Il trattamento dei dati da parte dei docenti avviene esclusivamente con mezzi manuali su supporti cartacei.

Le banche dati contenenti documentazione didattica (registri personali e di classe) vengono consegnati all'inizio dell'anno scolastico dal Dirigente scolastico ai docenti, che provvedono alla compilazione, alla conservazione ed alla custodia.

All'interno delle banche dati di cui si tratta vengono custoditi temporaneamente, in attesa del trasferimento nei fascicoli personali, i certificati medici degli alunni.

Le banche dati contenenti documentazione didattica vengono consegnate dai docenti al dirigente scolastico alla fine dell'anno scolastico.

I documenti di valutazione degli allievi vengono compilati dai docenti e custoditi e conservati dal personale di segreteria.

Gli elaborati degli alunni sono conservati in appositi contenitori nelle sale insegnanti ed alla fine di ogni anno scolastico sono consegnati dai docenti al personale di segreteria.

I verbali dei consigli di classe e la programmazione didattica di pertinenza sono custoditi e conservati dal Dirigente Scolastico.

La programmazione didattica per gli allievi diversamente abili è custodita e conservata dal Dirigente Scolastico. Per la descrizione puntuale della situazione dei locali siti presso la sede centrale di P.za Dante Alighieri si rimanda ai punti successivi. La situazione nelle sedi staccate ha una serie di caratteri comuni:

- modesta sicurezza delle vie di accesso (porte di ingresso di modesta consistenza e dotate di serrature ordinarie; presenza di numerose vie di accesso: porte di sicurezza, finestre non protette etc.)
- mancanza di adeguato sistema di allarme (scuola dell'Infanzia)
- arredi della sala insegnanti privi di serrature efficienti.

7.1.3 Locali dove avviene il trattamento effettuato dal Dirigente Scolastico e dal personale ATA

I locali interessati al trattamento dei dati da parte del personale di segreteria e da parte del dirigente scolastico sono collocati al piano terreno della sede principale di P.za Dante Alighieri - Pitigliano.

7.1.4 Descrizione generale dell'edificio che ospita presidenza e segreteria

L'edificio della sede centrale, è situato presso la scuola primaria di Pitigliano, in Piazza D. Alighieri 19, nel centro del paese. I locali relativi al trattamento dei dati da parte del personale di segreteria e del dirigente scolastico sono costituiti da:

- Direzione
- Segreteria
- Archivio
- Locali degli assistenti amministrativi

Descrizione dei locali

L'edificio posto al centro del paese è composto da un piano interrato, da un piano terreno rialzato e da un primo piano.

L'edificio è isolato dagli altri e attualmente è adibito a scuola primaria; la zona prospiciente l'istituto non è recintata.

L'edificio presenta al piano rialzato numerose finestre non dotate di sistemi antintrusione. Gli accessi all'edificio sono due su lati diversi costituiti da una porta con infissi e grate in alluminio con serratura ordinaria; l'ingresso di piazza D. Alighieri è controllato a vista dai collaboratori scolastici che presidiano il corridoio principale. Gli uffici amministrativi e il laboratorio sono protetti da un sistema di allarme.

7.1.5 Descrizione dei locali della Direzione e dei Servizi Amministrativi

I locali, posti in uno stesso corridoio, sono collocati al piano rialzato cui si accede tramite una scala proveniente dal piccolo atrio collocato al livello del manto stradale (accesso dalla P.za D. Alighieri)

- tramite una porta a vetri che dà sul retro dell'edificio, lato scala di emergenza,
- tramite una porta a vetri che dà attraverso i locali della palestra sul retro dell'edificio

Sul corridoio si affacciano locali adibiti ad attività didattica, sala informatica e servizi igienici ed una scala ed un ascensore che conducono al piano superiore.

I locali di cui si tratta sono: presidenza, segreteria, ufficio assistenti amministrativi.

Direzione e servizi di segreteria

I locali che ospitano la direzione, segreteria e uffici degli assistenti amministrativi sono posti al piano rialzato con porte che danno sul corridoio interno dell'edificio e finestre con ampie vetrate. In uno dei tre locali è presente un armadio blindato.

La direzione è arredata come gli uffici, non ci sono cassaforti o armadi blindati, ma armadi con normali chiusure a chiave. Detti locali sono protetti da adeguato sistema di allarme.

Archivio

L'Archivio è ubicato al primo piano in locale idoneo dal punto di vista del rischio incendi con porta tagliafuoco provvista di serratura ordinaria; il locale è provvisto di due finestre.

I documenti sono conservati in cartelle e faldoni.

A seguito di differenti dimensionamenti fra istituzioni scolastiche, alcuni fascicoli docenti continuano ad essere conservati nell'archivio dell'Istituto Comprensivo di Sorano.

Per tutti i locali:

- gli infissi non presentano particolari condizioni di sicurezza, non sono presenti sbarre alle finestre; i vetri delle finestre sono di tipo comune.
- Nell'aula multimediale e nei locali della segreteria e della direzione è installato un sistema di allarme.
- Le porte di accesso sono dotate di normali serrature; anch'esse non presentano particolari elementi di sicurezza.
- Per quanto riguarda il pericolo incendi o allagamento si fa riferimento al piano di sicurezza dei luoghi di lavoro ai sensi del Dlgs 626/94 conservato nella sede scolastica.
- Nei locali degli assistenti amministrativi sono presenti alcune postazioni di lavoro con casseti e armadi in metallo con serrature a chiave. Le banche dati contenenti dati personali e sensibili sono custodite in armadi e schedari metallici dotati di serratura collocati all'interno degli uffici.

7.1.6 Gestione delle chiavi

Chiavi per l'accesso all'edificio della Sede principale (P.za Dante Alighieri):

a) soggetti cui sono affidate le chiavi

personale istituzione

- Dirigente
- Direttore SGA
- Collaboratori scolastici

soggetti esterni

- nessuno

b) modalità di affidamento delle chiavi

- tramite verbali di consegna

c) esistono copie delle chiavi: **si**

custodite dal:

- Dirigente Scolastico e Direttore SGA
- Personale Collaboratore scolastico

Gestione delle chiavi di accesso ai locali dove sono trattati dati personali (Sede principale - P.za Dante Alighieri):

a) soggetti cui sono affidate le chiavi

personale istituzione

- dirigente scolastico
- direttore S.G.A.
- collaboratori scolastici del plesso.

soggetti esterni

- nessuno

- b) modalità di custodia delle chiavi
 - Bachecca nell'ufficio di segreteria
- c) esistono copie delle chiavi: **si**
 - custodite nell'armadio metallico dell'ufficio

Gestione delle chiavi degli archivi dove sono custoditi dati personali (Sede principale - P.za Dante Alighieri):

L'archivio attiguo all'ufficio degli assistenti amministrativi è dotato di serratura tipo Yale

- a) soggetti cui sono affidate le chiavi
 - dirigente scolastico
 - direttore S.G.A.
 - collaboratori scolastici del plesso.

soggetti esterni

 - nessuno
- b) modalità di custodia delle chiavi
 - custodite nell'armadio metallico dell'ufficio
- c) esistono copie delle chiavi: **si**

custodite dal:

 - Dirigente Scolastico e Direttore SGA
 - Personale Collaboratore scolastico

7.1.7 Gestione delle chiavi di accesso ai locali delle sedi staccate

Nelle sedi staccate (scuola dell'infanzia e scuola secondaria di primo grado) le chiavi di accesso ai locali sono affidate a tutti collaboratori scolastici e ai docenti collaboratori del dirigente scolastico.

Copie delle chiavi di cui si tratta sono custodite presso la sede centrale nell'armadio metallico dell'ufficio degli assistenti amministrativi.

7.2 Rilevazione struttura sistema informativo

- 1) Tipologia della rete
 - rete unica per i servizi amministrativi
- 2) Tipologia delle risorse hardware
 - n. 1 server
 - n. 5 P.C. in rete
- 3) Collocazione server
 - Locale segreteria
- 4) Accesso alle risorse Internet
 - Sì, tramite linea ADSL Alice
- 5) Posta elettronica e web
 - sì
 - provider casella elettronica ministeriali: gric82000e@istruzione.it
 - casella pec: comprensivopitigliano@pec.it
 - dominio: www.comprensivopitigliano.it

Tipologia delle risorse software

- 6) Sistema operativo usato sul server
 - WINDOW 2000 server
- 7) Sistemi operativi usati sui client
 - S.O. WINDOW XP
 - Microsoft Office Professional

- Procedure Alunni, personale, nuovo bilancio, inventario, stipendi, libri di testo, fisco (sissi – sidi programmi MIUR). Protocollo Argo Software.

8) Supervisore di rete

- consulenza con ditte esterne

9) Uso della rete

- condivisione programmi e risorse interne

10) Interventi di formazione del personale

- si

11) Assegnazione di nomi logici per le periferiche di rete

- si

12) Assegnazione della password di accesso alle singole macchine

- si

13) Assegnazione dei codici identificativi personali

- si

14) Collaboratori esterni o temporanei che hanno accesso alla rete personale

- no

Prevenzione della perdita dei dati

15) Incarico formale dell'esecuzione dei backup

- si incarico formale

16) Software antivirus

- avira antivirus

17) Supporto sul quale viene effettuato il backup

- Su hard disk
- su CD
- su pendrive

18) Libro mastro della programmazione dei backup

- si

19) Gruppo di continuità

- si

20) Manutenzione delle risorse hardware e software

- Ditta esterna incaricata. Vedi apposita convenzione.

ARTICOLO 8 **DIRITTI DELL'INTERESSATO**

L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, come pure l'aggiornamento, la rettifica o, quando vi ha interesse, l'integrazione dei dati.

L'interessato ha altresì diritto di richiedere la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge.

I dati saranno resi noti solo ai diretti interessati e a persone, enti e organismi che per legge sono titolari a ricevere i dati stessi.

Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali (D.L.vo 196/2003). Pertanto per adempiere ai doveri d'ufficio, a disposizioni normative, a precisi obblighi di circolari non si

richiede il consenso dell'interessato per l'invio di dati a persone od organismi titolari per legge a ricevere i dati stessi.

I dati sensibili possono essere oggetto di trattamento solo con il consenso scritto dell'interessato.

ARTICOLO 9

MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI, NONCHE' LA PROTEZIONE DELLE AREE E DEI LOCALI

1. MISURE DA ADOTTARE

Al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti al fini della loro custodia ed accessibilità, sono state adottate le seguenti misure:

- Individuazione e nomina del responsabile del trattamento dei dati (per l'accesso ai computer e alla rete si richiede password per ogni Incaricato);
- Misure di prevenzione per eliminare gli eventuali incendi con adeguate modalità di gestione degli stessi (impianto elettrico a norma, idranti (ove disposti), estintori, etc.);
- Individuazione dei locali e contenitori (armadi, armadi di sicurezza, armadi blindati, classificatosi con serrature, apparecchiatura e strumenti di raccolta dei dati adeguati e sicuri, etc.);
- Regolamentazione sia per il personale che per gli esterni nell'accesso ai locali e alle attrezzature che conservano dati, archivi e documentazione,
- Attuazione di misure di protezione attiva e passiva dei locali (porte con serrature di sicurezza, inferriate, archivio, sistemi di allarme ove collocati, adeguate misure antincendio con raccolta di materiali in locali protetti da porte specifiche di sbarramento);
- Periodico salvataggio dei dati del server su unità removibili
- Periodicamente (almeno ogni tre mesi) verificare la funzionalità e l'efficienza delle misure di protezione e delle strutture operative che ne hanno la responsabilità, anche mediante la compilazione di apposite schede di monitoraggio.
- Installazione di Firewall, già presente in Windows XP, al fine di impedire ingressi di pirati o intercettazioni sulla rete informatica di questa istituzione scolastica con la configurazione di password e impostazione di tutte le misure di sicurezza necessarie

2. CRITERI, PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI

Il Responsabile del trattamento, con il supporto dell' Amministratore di Sistema, stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche di dati trattati.

In particolare per ogni banca di dati devono essere definite le seguenti specifiche:

- Il tipo di supporto da utilizzare per le copie di back-up;
- Il numero di copie di back-up effettuate ogni volta;
- Verificare se i supporti utilizzati per le copie di back-up sono riutilizzati e in questo caso con quale periodicità;
- Concordare preventivamente se per effettuare le copie di back-up si utilizzino procedure automatizzate e programmate;
- Valutare la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- Assegnare il compito periodico di effettuare le copie di back-up agli Incaricati del trattamento;
- Verbalizzare su apposito registro l'avvenuta effettuazione del backup.

3. ADEGUAMENTI PREVISTI

A supporto del sistema di allarme deve essere prevista l'installazione di vetri antisfondamento o sbarre alle finestre e adeguate serrature alle porte negli uffici dei servizi amministrativi.

- Ogni posto di lavoro ove opera un incaricato del trattamento dati deve essere dotato almeno di un contenitore con serratura efficiente e sicura; per i docenti possono essere previste cassettiere dotate di serratura per ogni cassetto.
- Le banche di dati personali (sensibili e non) devono essere contenute in schedari o armadi dotati di serratura efficiente e sicura.
- I locali che contengono banche di dati personali (sensibili e non) e strumenti informatici devono essere dotati di una porta adeguata con serratura efficiente e sicura.
- Devono essere indicati all'interno dei locali amministrativi le zone interdette al pubblico o al personale estraneo agli uffici.
- Uso costante del dispositivo di back-up ed uso di un registro per l'annotazione periodica del salvataggio dati.
- Uso del gruppo di continuità e tenuta del registro dei controlli periodici di funzionamento dello stesso.
- Aggiornamento periodico del programma antivirus almeno sulle postazioni contenenti dati personali o sensibili.
- Autorizzazione e regolamentazione all'uso degli strumenti di telecomunicazioni, rete ADSL

4. CUSTODIA E CONSERVAZIONE DELLE COPIE DI BACK-UP

Le copie di back-up devono essere adeguatamente conservate a cura del Responsabile del trattamento nell'armadio blindato sito in segreteria. Tale sito di custodia delle copie di back-up è protetto da:

- Agenti chimici
- Fonti di calore
- Campi magnetici
- Intrusioni ed atti vandalici
- Allagamento
- Furto
- Condizionamento ambientale
- Impianti elettrici a norma e gruppi di continuità

Dal momento che detto armadio non è in grado di proteggere le copie di back-up in caso di incendio si provvederà a conservare una seconda copia del back-up in altri locali.

L'accesso ai supporti utilizzati per il back-up dei dati è limitato:

- Al Titolare del trattamento
- Al Responsabile del trattamento della sicurezza dei dati All'Amministratore di Sistema.
- Agli Incaricati

5. PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita degli stessi a causa di virus informatici, il Responsabile del trattamento dei dati stabilisce, con il supporto dell'Amministratore di sistema che cura il back-up, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Il Responsabile del trattamento stabilisce inoltre la periodicità, con cui devono essere effettuati gli aggiornamenti dei sistemi antivirus utilizzati per ottenere un accettabile standard di sicurezza dei dati trattati

E' consigliabile che gli Incaricati che utilizzano i sistemi informatici annotino gli 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.

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezioni o contagio da virus, il Responsabile del trattamento, unitamente all'Amministratore di Sistema, deve provvedere a:

- Isolare il sistema
- 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 i sistemi
- Compilare un modulo di "Report dei contagi da virus informatici"
- Conservare in luogo sicuro a cura del Responsabile del trattamento i moduli compilati.

6. PROTEZIONE DELLE AREE E DEI LOCALI

Sicurezza di area

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze nello svolgimento dei servizi. Le contromisure si riferiscono alla protezione perimetrale dei siti, ai controlli fisici all'accesso, alla sicurezza degli archivi e delle attrezzature informatiche rispetto ai danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti. L'edificio scolastico dove ha sede la Presidenza non è protetto da inferriate. Tutte le scuole sono dotate di impianto elettrico a norma e di appositi estintori. La Scuola Primaria e la Scuola Secondaria sono dotate di impianto di allarme con sirena e commutazione telefonica con i carabinieri.

Si precisa inoltre che:

- nessuno accede all'archivio se non autorizzato
- i fascicoli prelevati dall'archivio permangono al di fuori del sito per il tempo strettamente necessario e successivamente vengono riposti al proprio posto gli incaricati accedono ai soli dati personali la cui conoscenza sia strettamente necessaria per evadere una pratica
- i supporti non informatici contenenti la riproduzione di informazioni relative al trattamento devono essere conservati e custoditi con le necessarie precauzioni.

ARTICOLO 10

CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

- 1) Per prevenire e diminuire i danni causati da danneggiamento, smarrimenti, inaffidabilità della base dati:
 - a) per i dati cartacei si potrà ricostruire copia da documenti e atti in possesso degli interessati (Personale in genere) o di altri enti cui sono stati trasmessi (Scuole, MIUR, Ufficio Scolastico Regionale, CSA, ASL, Comune);
 - b) per i dati informatici si potranno ricostruire i dati danneggiati ricavando gli stessi da atti e documenti "stampati" o si potranno riportare in via precauzionale su supporti di memoria custoditi in luoghi fisici diversi i dati contenuti negli archivi informatici fissi.
- 2) Ogni Incaricato della gestione di dati avrà l'accortezza di effettuare periodicamente il salvataggio dei dati dalle copie di back-up custoditi dallo stesso.
- 3) Il Responsabile del trattamento, d'intesa con gli Incaricati di collaborare nell'Amministrazione di Sistema, ha il compito di verificare di sovente o almeno ogni sei mesi 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:
 - La sicurezza dei dati trattati
 - Il rischio di distruzione o di perdita dei dati
 - Il rischio di accesso non autorizzato o non consentito
- 4) Per evitare danneggiamento o perdita di dati si rende estremamente importante:
 - La disponibilità delle versioni più avanzate dei Sistemi Operativi utilizzati
 - L'aggiornamento del Sistema (System-Pack) per la rimozione di errori o malfunzionamenti

- Nel caso esistano evidenti rischi sui Sistemi operativi, l'amministratore di sistema e il Responsabile informano il Titolare perché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme in vigore ad evitare che possano essere smarriti, danneggiati o distrutti.

ARTICOLO 11

INTERVENTI FORMATIVI PER GLI INCARICATI DEL TRATTAMENTO

Ai Responsabili del trattamento dei dati è affidato il compito di verificare ogni anno i bisogni formativi di cui necessitano gli Incaricati, specie per le innovazioni che nel campo telematico/tecnologico/informatico avvengono di continuo. E' necessario tenere il personale in tale campo continuamente informato e all'altezza dei compiti che devono espletare, per meglio conoscere i rischi che incombono sui dati, per avere una ottimale conoscenza delle misure di sicurezza e degli adeguati comportamenti da adottare, delle responsabilità circa i dati danneggiati, persi o distrutti.

Gli interventi formativi sono particolarmente opportuni al momento dell'ingresso in servizio di personale nuovo, per immissione in ruolo o per trasferimento, in occasione dell'adozione di nuovi strumenti o dell'installazione di altri software. E' opportuno documentare gli interventi formativi.

Gli interventi formativi atterranno sulle disposizioni applicative del D.L.vo 196/2003 e dal Decreto 7 dicembre 2006, n. 305 e su tutte le successive modifiche e integrazioni.

Il personale tutto, docente e non docente, ha fruito di una formazione iniziale che risale agli anni precedenti. Sono comunque previsti interventi informativi e formativi sugli aggiornamenti normativi mediante opuscoli per l'autoformazione e interventi di formazione in aula con il metodo delle lezioni frontali.

A tutti gli Incaricati del trattamento al momento della presa in servizio verrà data comunicazione informativa sulla normativa vigente, sugli obblighi di Legge relativamente all'affidamento dei compiti e delle responsabilità comunque entro il primo semestre di ciascun anno scolastico. Per il personale tutto sarà messo a disposizione per la visione il D. L vo 196/2003 e il Decreto 7 dicembre 2006, n. 305.

ARTICOLO 12

NORME FINALI

Il "DPS" potrà essere integrato e aggiornato in qualunque periodo dell'anno, ma almeno entro il 31 marzo di ogni anno.

Per quanto non regolamentato nel presente DPS si applicano le norme contenute nel D.L.vo 196/2003 e dallo stesso richiamate.

Il D.S. - 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 destinata a salvaguardare la sicurezza dei dati personali, siano essi contenuti nei documenti cartacei che registrati mediante strumenti elettronici. Tali misure riguarderanno gli aspetti organizzativi, logistici e procedurali miranti ad evitare con ogni mezzo qualsiasi incremento di rischio di distruzione o perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito.

Il presente documento verrà portato all'attenzione del Consiglio di Istituto nella prima seduta utile, con gli opportuni adeguamenti che deriveranno dalla verifica annuale dell'assegnazione degli incarichi e delle specifiche competenze, come previsto dall'allegato B, n. 26 sul Disciplinare tecnico in materia di misure minime di sicurezza, per informazione ai componenti, anche al fine di porre il Titolare in grado di attuare gli adeguamenti fisici, logistici, tecnologici ed informatici urgenti e necessari per le finalità previste dalla legge.

Pitigliano li, 9 marzo 2011

Titolare del trattamento dei dati

Il Dirigente scolastico
(*Prof.ssa. Daniela Busoni*)