DOCUMENTO PROGRAMMATICO SULLA SICUREZZA DEI DATI

(ai sensi del D.Lgs. 196/2003)

revisione di marzo 2011

LICEO GINNASIO STATALE

"Mariano Buratti"

Via Tommaso Carletti n.8 - Viterbo (VT)
C.F. 80014070561

INDICE

7. **Modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento**

8. **Interventi formativi**
   - 8.1 Interventi formativi già attuati
   - 8.2 Interventi formativi al momento dell'ingresso in servizio
   - 8.3 Interventi formativi di aggiornamento

9. **Misure specifiche per i dati personali idonei a rivelare lo stato di salute**

10. **Formalizzazione del documento**

Allegati

A – documenti di nomina per l'assegnazione di responsabilità ed incarichi
B – lista degli incaricati di trattamento con strumenti elettronici
C – lista degli incaricati di trattamento senza l'ausilio di strumenti elettronici

1 - INTRODUZIONE

Il presente documento (DPPS) definisce lo stato di attuazione, per il Liceo Ginnasio Statale "Mariano Buratti" Via Tommaso Carletti n.8 - Viterbo (VT), C.F. 80014070561, di quanto previsto dal D. Lgs. 30 giugno 2003 n° 196 Codice in materia di protezione dei dati personali agli articoli 31, 33, 34 e 35 e dal Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Codice).
Per la suddetta istituzione Scolastica il **Titolare del Trattamento Dati** è il Dirigente Scolastico:

Prof.ssa PAOLA MOSCUCCI

Il contenuto di quanto segue si riferisce alla struttura organizzativa e funzionale della istituzione scolastica che prevede il trattamento di dati effettuato, per le rispettive competenze, dal corpo docente e dal personale ATA. Nell'affrontare e risolvere le varie problematiche riferite all'applicazione *Disciplinare tecnico in materia di misure minime di sicurezza (allegato B del Codice)* si è ritenuto opportuno quindi considerare, all'interno di uno stesso quadro organizzativo, in modo separato il trattamento dei dati operato dal personale docente e dal personale ATA.

I dati personali, comuni e sensibili, trattati da docenti riguardano essenzialmente gli alunni; i dati personali, comuni e sensibili trattati dal personale di segreteria riguardano sia gli alunni che il personale della scuola.

2 - ELENCO DEI TRATTAMENTI DI DATI PERSONALI

2.1 Dati trattati dal personale docente

I dati personali trattati dai docenti sono contenuti in banche dati su supporto cartaceo che si possono classificare in:

- **basi di dati alle quali hanno accesso più docenti**
- **basi di dati alle quali ha accesso un singolo docente.**

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
- i certificati medici degli allievi
- la corrispondenza con le famiglie

Le banche dati cui ha accesso il singolo docente sono:

- il registro personale
- gli elaborati

Appare opportuno considerare i dati trattati dai docenti nel loro insieme come dati sensibili, ai sensi del comma 1, lettera d del D. Lgs. 196/2003 essendo difficile, per loro natura e organizzazione, classificarli in sensibili e personali. 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.

2.2 Dati trattati dal personale ATA

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

- i fascicoli relativi al personale della scuola,
- i fascicoli alunni ed ex alunni
- l'anagrafe fornitori, i contratti
- documentazione finanziaria e contabile
- la documentazione didattica trattata dai docenti per la conservazione
- il registro degli infortuni
- il registro di protocollo
- gli atti e i documenti prodotti dalla Istituzione

2.2 Dati trattati dal dirigente scolastico

Le banche dati di esclusiva pertinenza del Dirigente Scolastico sono:

- il fascicolo del personale direttivo
- i verbali delle assemblee dei genitori
- la programmazione relativa allo stato di disagio.
- il protocollo riservato
- il fascicolo del personale in prova.

3 - DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ

Il codice individua i soggetti che sono coinvolti nel trattamento dei dati personali:

- il **titolare,** cioè la persona fisica o giuridica che ha la responsabilità finale ed assume le decisioni fondamentali riferite al trattamento dei dati personali;

- il **responsabile**, è la persona, dotata di particolari caratteristiche di natura morale e di competenza tecnica, preposta dal titolare al trattamento dei dati personali "ivi compreso il profilo della sicurezza"; possono essere nominati anche più responsabili in base ad esigenze organizzative;

- l'**incaricato** è la persona fisica che materialmente provvede al trattamento dei dati, secondo le istruzioni impartite dal titolare o dal responsabile se nominato;

- l'**interessato**, è il soggetto cui i dati oggetto di trattamento si riferiscono.

Il DPR 318/99 individuava ,all'articolo 1, un altro soggetto che si aggiungeva ai quattro elencati in precedenza:

- l'**amministratore di sistema,** 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".

Il Codice non contempla tale soggetto che comunque può essere ricondotto ad un tipo particolare di incaricato avente come necessaria caratteristica opportune competenze tecniche.

3.1 Individuazione ed attribuzioni del responsabile

Per la individuazione del responsabile, la cui nomina è facoltativa, esistono diverse possibilità:

a) non viene nominato, ed il dirigente scolastico assume personalmente tutte le incombenze relative agli adempimenti previsti dal D.Lgs.196/2003 per il titolare;
b) viene nominato il direttore dei servizi generali ed amministrativi per i trattamenti dei dati che riguardano in modo specifico i servizi di segreteria mentre il dirigente scolastico si occupa direttamente del trattamento dei dati effettuato dai docenti;
c) vengono nominati:
   - il direttore dei servizi generali ed amministrativi per i trattamenti dei dati che riguardano in modo specifico i servizi di segreteria;
   - uno o più docenti per i trattamenti dati effettuati dagli insegnanti per fini didattici.

In base a quanto disposto dall art 29 2° comma, D.Lgs.196/2003
" Il responsabile se designato, deve essere nominato fra i soggetti che per esperienza capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza".

Il dirigente scolastico ha deciso di adottare la soluzione "b" dato che fino al momento attuale le questioni afferenti all'accesso ai documenti da parte degli interessati sono state trattate, per le rispettive competenze, dallo stesso e dal direttore dei servizi generali ed amministrativi e visto che la individuazione di docenti come responsabili richiederebbe la preventiva realizzazione di impegnative attività di formazione
Viene quindi individuato come responsabile, per i trattamenti dei dati che riguardano in modo specifico i servizi di segreteria, il direttore dei servizi generali ed amministrativi nella persona di

SCALZINI MARIA TERESA

3.2 I Responsabili esterni

nessuno

3.3 Gli Incaricati

Il docente **è da considerarsi, per la propria sfera di competenza, incaricato del trattamento come tale deve essere nominato mediante specifico atto che elenchi puntualmente: categorie dei dati cui può avere accesso; tipologia di trattamento e vincoli specifici applicabili alle varie tipologie di dati; istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.**

Ogni **assistente amministrativo** dovrà essere nominato incaricato del trattamento con specifico atto, in base ai compiti che assolve nell'ufficio.

I **collaboratori scolastici**, qualora trattino anche saltuariamente dati personali, dovranno essere incaricati con specifico atto.

Le nomine di incaricato del trattamento dati saranno effettuate anche per il **personale supplente temporaneo, docente e ATA** .

Dovrà essere nominato incaricato anche il personale esterno (persone fisiche) che sulla base di incarichi o convenzioni stipulate con l'Istituzione scolastica ha accesso al trattamento di dati personali, compreso il **personale esterno incaricato della manutenzione degli strumenti informatici.**.

Nello specifico verrà valutata la possibilità di ricorrere a risorse interne. Nel caso in cui ciò non fosse possibile si verificherà la possibilità di nominare personale esterno. Si procederà quindi alla nomina appena individuata la persona più adatta .

4 - ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

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

4.1 Situazione attuale

I dati che seguono sono relativi a una rilevazione effettuata nel mese di marzo 2011

Personale/lavoratori	**n°**
Docenti	**84**
Personale di segreteria + Assistente Tecnico	**9**
Collaboratori scolastici	**12**

Locali contenenti dati personali o sensibili	**n°**
Presidenza	**1**
Adibiti a uso amministrativo	**1**
Archivi	**1**

4.1.1 Plessi e loro collocazione

SEDE PRINCIPALE Istituto Presidenza e uffici di segreteria	Via Tommaso Carletti n.8 C.F. 80014070561	Viterbo

4.1.2 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.

Esistono 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 e sono consegnarti dai docenti al personale di segreteria periodicamente.
I verbali dei consigli di classe e la programmazione didattica di pertinenza sono custoditi e conservati dal D.S.
La programmazione didattica per gli allievi portatori di handicap è custodita e conservata dal D.S.
Per la descrizione puntuale della situazione dei locali siti presso la sede centrale si rimanda ai punti successivi. In generale comunque la situazione è la seguente:

- 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 un sistema di allarme,
- arredi della sala insegnati non dotati di serrature efficienti.

4.1.3 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 nella sede principale in due locali contigui al primo piano di un edificio storico.

SEDE	Direzione, Segreteria Archivio	Via Tommaso Carletti n.8	Viterbo

4.1.4 Descrizione generale dell'edificio che ospita presidenza e segreteria

L'edificio della sede centrale è situato nel pieno centro di Viterbo in un edificio storico.

L'edificio è posto su due piani. Entrambi non presentano accessi dall'esterno facilmente controllabili .

Accesso	N° 1 principale
Recinzione	no
cortile / giardino esclusivo	no
parcheggi esclusivi	no
cancelli esterni di accesso	no
illuminazione esterna	no
piani interrati	no
sistema generale di allarme	non presente
locali utilizzati da altri soggetti	no

4.1.5 Descrizione dei locali della Direzione e dei Servizi Amministrativi

I locali si affacciano sullo stesso corridoio, sono collocati al piano superire cui si accede

- tramite l'atrio principale, una scalinata e porta di piano non sicura .

Tutti i locali sono dotati di porte con serrature ordinarie.
Negli uffici amministrativi sono presenti armadi senza adeguata chiusura contenenti documentazione varia (fascicolo alunni e personale)
In un altro armadio metallico chiuso con chiave in possesso degli operatori ci sono le pubblicazioni. Anche per il locale Presidenza non abbiamo dotazioni particolari per la sicurezza fisica di area.

ARCHIVIO AMMINISTRATIVO E STORICO
In locale con accesso dal corridoio, con estintore , con finestra senza grate. L'arredo interno è costituito da scaffali in metallo. Nell'archivio sono conservati i:

- fascicoli alunni
- compiti in classe
- materiale del Consiglio di Istituto
- relazioni e protocollo storico.

4.1.6 Gestione delle chiavi

Chiavi per l'accesso all'edificio della Sede di via Tommaso Carletti VT

a) soggetti cui sono affidate le chiavi

personale istituzione

- Dirigente - tutte
- Direttore SGA - tutte
- Collaboratori scolastici

soggetti esterni

- nessuno

b) modalità di affidamento delle chiavi

- informale sono in corso verbali di consegna

c) esistono copie delle chiavi

d) in caso di risposta positiva indicare il soggetto o i soggetti preposti alla custodia delle copie di sicurezza

- Dirigente e Direttore SGA

Gestione delle chiavi di accesso ai locali dove sono trattati dati personali

Locali situati nell'edificio

a) soggetti cui sono affidate le chiavi

- collaboratori scolastici
- assistenti amministrativi

soggetti esterni

- - nessuno

b) modalità di custodia delle chiavi

- bacheca nel locale della segreteria

c) esistono copie delle chiavi :

si

d) in caso di risposta positiva indicare il soggetto o i soggetti preposti alla custodia delle copie di sicurezza

- D.S. e D.S.G.A.

Gestione delle chiavi degli archivi dove sono custoditi dati personali

Archivi situati nei locali

- Tutti i locali dei settori amministrativi
(uffici ed archivi così come precedentemente descritti)

a) soggetti cui sono affidate le chiavi

Le chiavi di accesso all'edificio sono affidate ai Collaboratori Scolastici
Le chiavi di accesso agli archivi e agli armadi/cassetti con serratura sono affidate esclusivamente agli Assistenti Amministrativi
La chiavi per accedere ai luoghi ove è il protocollo riservato e altri dati sensibili sono in possesso esclusivamente del Titolare e del Responsabile del Trattamento

b) esistono copie di sicurezza delle chiavi
si

4.1.7 Rilevazione struttura sistema informativo

1-Tipologia della rete
- *rete unica , intranet, per i servizi amministrativi*
- *posta elettronica: ministeriale e altro provider*

2- Tipologia delle risorse hardware

PC in rete

Tipologia delle risorse software

6- Sistema operativo usato sul server
- *WINDOW XP*

7-Sistemi operativi usati sui client
Programmi:

Vedi relazione tecnica allegata

8- Supervisore di rete

non presente

9- Progetto e certificazione della rete
Non presente

10- Planimetria della rete

Non presente

11- Uso della rete
- *condivisione programmi e risorse interne*

12- Interventi di formazione del personale
- *Si*

13- Assegnazione di nomi logici per le periferiche di rete
- *Si*

14- Assegnazione delle password di accesso alle singole macchine
- Si

15- Assegnazione dei codici identificativi personali

- *in fase di attuazione*

16- Collaboratori esterni o temporanei che hanno accesso alla rete personale a convenzione
- *nessuno*

Prevenzione della perdita dei dati

17- Incarico formale dell'esecuzione dei backup
- *incarico formale ad un incaricato*

18- Software antivirus
- Installato e periodicamente aggiornato

19- Supporto sul quale viene effettuato il backup
- su CD

20- Libro mastro della programmazione dei backup
- *in via di approntamento*

21- Gruppi di continuità
- si

22- Manutenzione delle risorse hardware e software
- *ditte esterne a chiamata e fornitori software a convenzione*

4.2 Analisi dei rischi

Si metteranno di seguito in evidenza i rischi propri, connessi al trattamento dei dati personali; tali rischi si possono classificare in:
- distruzione o perdita, anche accidentale dei dati;
- connessi alla integrità dei dati;
- accesso non autorizzato ai dati;
- trattamento non consentito o non conforme alla finalità della raccolta;
- connessi con l'utilizzo di reti di telecomunicazione disponibili al pubblico;
- connessi alla conservazione della documentazione relativa al trattamento;
- connessi all'utilizzo di archivi e contenitori con serrature.

4.2.1 Rischi riguardanti le basi di dati trattate da docenti

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

- **distruzione o perdita accidentale dei dati** a causa di eventi naturali, allagamenti, furto danneggiamento etc.:

il rischio appare presente ma non particolarmente rilevante dato che i documenti contenenti dati personali trattati da docenti sono in gran parte affidati agli stessi e restituiti alla fine del trattamento; fra le banche dati trattate da docenti che permangono nella scuola appare a rischio il registro di classe se non debitamente custodito

- **connessi alla integrità dei dati**: utilizzo di supporti o modalità di trattamento non stabili;

  rischio nel complesso irrilevante data la tipologia dei supporti cartacei utilizzati

- **accesso non autorizzato ai dati,** da parte di soggetti esterni alla scuola o da parte di personale interno;

  il rischio appare presente e di media entità data la presenza di contenitori non adeguati nelle sale docenti e la dislocazione di tali contenitori in luoghi non idonei(il più delle volte aperti al pubblico)

- **trattamento non consentito o non conforme** alle finalità di raccolta: diffusione, comunicazione, manomissione,

  rischio nel complesso basso vista l'esperienza del personale, le procedure adottate e le iniziative di formazione

- **connessi all'utilizzo di archivi e contenitori con serrature**

  rischio presente dato che nelle situazioni descritte in precedenza sono presenti contenitori ed archivi dotati di serrature inefficienti e/o non adeguate .

4.2.2 Rischi riguardanti le basi di dati trattate dal personale ATA

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

I rischi di cui si tratta sono:

- **distruzione o perdita accidentale dei dati** a causa di eventi naturali, allagamenti, furto, danneggiamento etc.;

  Data la collocazione dei locali il rischio di allagamento per cause naturali appare basso, come quelli dipendenti dal verificarsi di guasti alle condotte idriche e termiche.
  Relativamente ai rischi di furto e di danneggiamento:
  - *il rischio appare* medio *per gli uffici amministrativi e la presidenza durante l'orario di apertura, dato il presidio da parte del personale;*
  - *nel periodo di chiusura della istituzione scolastica i rischi relativi a furto e danneggiamento, appaiono medio/alti data la presenza di diverse vie di accesso.*
  - *i rischi sono presenti per gli archivi cartacei data la tipologie dello stesso .*

- **connessi alla integrità dei dati**: utilizzo di supporti o modalità di trattamento non stabili

  - per i dati su supporti cartacei il rischio è da considerarsi, nel complesso, ***medio*** *anche se si ritengono opportune verifiche periodiche*

- per i dati informatici il rischio è ***basso*** *dato che le copie di sicurezza, vengono eseguite su CD-rom*

- **accesso non autorizzato ai dati,** da parte di soggetti esterni alla scuola o da parte di personale interno

  - il rischio è presente e rilevante dato che, anche per cause strutturali dovute alla disposizione degli uffici e degli arredi ed alla la mancanza di regolamentazione degli accessi, soggetti interni ed esterni possono accedere ai documenti con relativa facilità;

- **trattamento non consentito o non conforme alle finalità di raccolta**: diffusione, comunicazione, manomissione

  - il rischio appare presente ma di non particolare rilievo in quanto il personale è esperto e consapevole delle proprie responsabilità;

- **connessi all'utilizzo di archivi e contenitori con serrature**

  - rischio presente dato che nelle situazioni descritte in precedenza sono presenti contenitori ed archivi dotati di serrature inefficienti e/o non adeguate

- **connessi all'utilizzo del sistema informativo automatizzato**

  Si veda relazione allegata

4.2.3 Analisi dei rischi per il sistema informativo automatizzato

nella individuazione degli elementi del sistema informativo automatizzato che necessitano di protezione e delle minacce cui gli stessi possono essere sottoposti, tenendo conto del fattore tecnologico e del fattore umano.

- **Risorse hardware**

Elementi da proteggere:
- CPU
- P.C.
- stampanti
- disk drive
- linee di comunicazione

Minacce cui sono sottoposti
- malfunzionamenti dovuti a guasti
- malfunzionamenti dovuti a sabotaggi
- malfunzionamenti dovuti ad eventi naturali
- malfunzionamenti dovuti a furti e intercettazioni

- **Risorse software**

Elementi da proteggere:
- Sistemi Operativi
- Software di Base

- Software Applicativi
- Gestori di basi di dati
- Software di rete

Minacce cui sono sottoposti

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

- **Dati**

  - Si tratta del contenuto degli archivi, delle base di dati, dati di transito, copie storiche, file di log, etc.

Minacce cui sono sottoposti

- accesso non autorizzato
- modifiche deliberate o accidentali

- **Risorse professionali**

  - Si tratta di operatori, addetti alla manutenzione, consulenti .

Minacce cui sono sottoposti

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

- **Supporti di memorizzazione**

  - Sono i supporti su cui vengono tenute le copie dei software installati, dei file di log e dei back-up.

Minacce cui sono sottoposti

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

5 - MISURE DA ADOTTARE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI

5.1 Misure fisiche

I requisiti di sicurezza fisica sono tesi a:

- proteggere le persone che operano sui sistemi,
- proteggere le aree
- proteggere gli archivi.

5.1.1 Sicurezza di area

La sicurezza di area ha il compito di prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi. Le contromisure si riferiscono alle protezioni perimetrali dei siti, ai controlli fisici all'accesso, alla sicurezza degli archivi e delle attrezzature informatiche rispetto a danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.
Come si evince da quanto descritto in precedenza (vedi "Situazione attuale") i locali, presentano problematiche di sicurezza relative a possibili intrusioni dall'esterno superate con l'installazione di un sistema di allarme.

Adeguamento 1

a) Messa in sicurezza delle vie di accesso ai locali amministrativi, porte esterne e finestre accessibili, della istituzione attraverso la installazione di adeguate protezioni (serrature efficienti, vetri antisfondamento e/o grate metalliche).

Per l'archivio è necessario individuare un locale idoneo con requisiti di sicurezza e antincendio adeguati (porta sicura con serratura efficiente, dispositivi anti intrusione per le finestre, dispositivo di rilevazione del fumo).

Adeguamento 2

a) Installazione in tutti gli edifici della istituzione scolastica di cassettiere con chiavi , per la custodia dei registri di classe.

5.1.2 Sicurezza degli archivi

Adeguamento 3

a) Ogni posto di lavoro ove opera un incaricato del trattamento dati deve essere dotato almeno di un contenitore (cassetto, armadio) con serratura efficiente e sicura;

Adeguamento 4

a) Tutte le banche di dati personali (sensibili e non) devono essere conservate in contenitori adeguati (schedari, armadi) dotati di serratura efficiente e sicura.

Adeguamento 5

a) I locali che contengono banche di dati personali (sensibili e non) e/o strumenti informatici devono essere dotati di una porta con serratura efficiente e sicura;

Adeguamento 6

a) Nei locali accessibili al pubblico dovrà essere delimitata l'area di accesso, ove non possibile l'accesso sarà consentito, attraverso idonee misure organizzative, solo in presenza del personale addetto

b) Dovranno essere indicati i locali interdetti al pubblico.

Adeguamento 7

a) La modalità di gestione delle chiavi deve essere resa sicura attraverso misure organizzative (verbali di consegna contenenti istruzioni dettagliate), individuazione o acquisizione di contenitori affidabili e sicuri (per collocazione o per accessibilità) per le chiavi che vengono custodite nella Istituzione.

5.1.3 Attuazione degli adeguamenti riferiti alle misure fisiche

Questa Istituzione scolastica per provvedere agli adeguamenti riferiti alla sicurezza delle strutture e degli arredi, descritte al punto precedente, non dispone di risorse finanziare proprie ma deve riferirsi all' Amministrazione provinciale alla quale si faranno specifiche richieste riferite al contenuto del presente documento.

5.2 Misure informatiche

Il campo di applicazione della Sicurezza Logica riguarda la protezione dell'informazione, e di conseguenza di dati, applicazioni, sistemi e reti, sia in relazione al loro corretto funzionamento ed utilizzo, sia in relazione alla loro gestione e manutenzione nel tempo.
Il Disciplinare tecnico in materia di misure minime di sicurezza, allegato B al Codice, prescrive l'adozione di alcune modalità tecniche che in questa Istituzione scolastica si sintetizzano come segue.

5.2.1 Sistema di autenticazione

Adeguamento 8
Devono essere rese operative per gli incaricati di trattamento (personale di segreteria) le credenziali di autenticazione.

Il sistema informatico attualmente in adozione presso questa Istituzione prevede, quale credenziale di autenticazione, un codice associato a una parola chiave.

La gestione del sistema di autenticazione informatica, per il personale di segreteria, sarà effettuato (disposto) dal responsabile come segue:

a) La parola chiave viene assegnata dal responsabile all'incaricato all'atto del primo conferimento dell'incarico.

b) La parola chiave è modificata dall'incaricato al primo utilizzo e, successivamente, almeno ogni sei mesi.

c) In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

d) La parola non deve contenere riferimenti agevolmente riconducibili all'incaricato.

e) Ad ogni modifica della parola chiave, la parola chiave scelta dall'incaricato è inserita in una busta sigillata con all'esterno dati identificativi dell'interessato e la data di consegna; la busta sarà consegnata al responsabile che la custodirà garantendo la segretezza del contenuto.

f) In caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema il responsabile potrà accedere alla credenziale; provvedendo ad avvertire tempestivamente l'incaricato.

5.2.2 Sistema di autorizzazione

La gestione del sistema di autorizzazione informatica viene effettuato dal responsabile.
I profili di autorizzazione sono individuati e configurati anteriormente all'inizio del trattamento.

5.2.3 Altre misure

a) Almeno annualmente è verificata da parte del responsabile la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

b) Il responsabile verifica annualmente la lista degli incaricati di trattamento e degli addetti alla gestione e manutenzione verificando l'ambito di trattamento consentito ed i relativi profili di autorizzazione.

c) Il responsabile dispone che i dati personali siano protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

d) Il responsabile impartisce istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale, attraverso il conferimento di uno specifico compito ad un incaricato e l'istituzione di un registro per il back-up.

e) Il responsabile provvede alla custodia in un luogo sicuro delle copie di back-up.

f) Il responsabile dispone la custodia dei supporti rimovibili contenenti dati personali individuando contenitori con idonee caratteristiche di sicurezza.

g) Il responsabile dispone la distruzione di supporti rimovibili contenenti dati sensibili e giudiziari non più utilizzati.

h) Il responsabile dispone e verifica la cancellazione di tutti i dati personali dagli strumenti informatici non più utilizzati o utilizzati in attività diverse da quelle amministrative.

i) Il titolare quando si avvarrà di soggetti esterni per la fornitura di prodotti o servizi finalizzati alla realizzazione di misure minime di sicurezza, si farà consegnare dal soggetto medesimo una descrizione scritta dell'intervento che ne attesti la conformità a quanto disposto dal disciplinare tecnico allegato B del Codice.

Adeguamento 9

a) Assegnazione delle password a tutti i P.C.

5.2.4 Attuazione degli adeguamenti riferiti alle misure informatiche

Per quanto attiene agli adeguamenti del sistema informatico descritti ai punti precedenti questa istituzione può provvedere nei tempi previsti dato che :

- A parte il software di gestione che non appare in linea con le norme e sarà oggetto di aggiornamento in tal senso, si tratta quindi solo di attivare le previste procedure di autenticazione;
- l'attivazione di idonei strumenti elettronici per prevenire il rischio di intrusione nel sistema informatico ha aspetti tecnici, organizzativi ed economici sostenibili;
- l'attivazione di idonei strumenti per prevenire la perdita dei dati è del pari realizzabile mediante misure organizzative e con modesti impegni economici (acquisto gruppo di continuità).

5.3 Misure organizzative

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

Gli aspetti organizzativi riguardano principalmente:
- la definizione di ruoli, compiti e responsabilità per la gestione di tutte le fasi del processo Sicurezza;
- l'adozione di specifiche procedure che vadano a completare e rafforzare le contromisure tecnologiche adottate.

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

In ordine alla norme di comportamento, si rimanda a quanto è definito nei documenti di nomina per l'assegnazione di responsabilità ed incarichi ed a quanto specificato nell'allegato A.

Il titolare ed il responsabile, relativamente ai propri ambiti di competenza, aggiornano almeno annualmente entro il mese di ottobre la lista degli incaricati (redatta anche per classi omogenee di incarico) con i relativi profili di autorizzazione utilizzando gli allegati B e C.

6 - CRITERI DA ADOTTARE PER GARANTIRE L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA NEL CASO DI AFFIDAMENTO DEL TRATTAMENTO A SOGGETTI ESTERNI

Nel caso di affidamento da parte della Istituzione a soggetti esterni di attività che comportino trattamento dei dati conviene distinguere due casi:

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

6.1 Affidamento a persone fisiche.

Nel caso che il soggetto sia una persona fisica lo stesso sarà nominato, dal titolare o dal responsabile, incaricato di trattamento dati attraverso un atto di nomina che specifichi puntualmente le norme di comportamento da seguire.
Ove necessario il titolare o il responsabile provvederanno a informare l'incaricato sui contenuti fondamentali delle norme che disciplinano il trattamento dei dati personali.
Il titolare o il responsabile verificheranno periodicamente, nelle forme ritenute più opportune, sulla correttezza del trattamento, con particolare riferimento all'adozione delle misure minime di sicurezza, da parte degli incaricati

6.2 Affidamento a persone giuridiche.

Nel caso che il soggetto sia una persona giuridica lo stessa sarà nominata dal titolare responsabile esterno di trattamento dati attraverso 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 dipendenti dal responsabile esterno e si farà rilasciare dallo stesso una dichiarazione di conformità a quanto stabilito dalle norme di legge e dal presente documento.

7 - MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

Il responsabile nel caso del verificarsi di eventi che provochino la distruzione od il danneggiamento dei dati personali contenuti nelle banche dati del sistema informatico, provvederà senza ritardo a ripristinare la funzionalità delle banche dati utilizzando le copie di back-up , stimando un tempo di ripristino dell'efficienza delle funzionalità quantificabile in una giornata lavorativa a meno di tempi di fornitura di hardware.

8 - INTERVENTI FORMATIVI

8.1 Interventi formativi già attuati

E' stata realizzata già realizzato nell'a.s. 2004/05 la formazione di tutto il personale della Istituzione in servizio, docente ed ATA, attraverso la organizzazione di una specifica attività. Il
Dirigente scolastico ed il Direttore SGA verranno sottoposti a specifica formazione.
Il personale supplente temporaneo che prenderà servizio durante il corso dell'anno scolastico verrà informato sui contenuti del codice e sui doveri da esso derivanti, anche attraverso la fornitura di materiale informativo di sintesi dal titolare o dal responsabile.

8.2 Interventi formativi al momento dell'ingresso in servizio

All'inizio di ogni anno scolastico, entro il mese di ottobre, il titolare ed il responsabile programmeranno, qualora necessario, attività formative per il personale che prende servizio nella istituzione e che non è stato in precedenza sottoposto a formazione sui temi di cui si tratta.
Gli interventi formativi potranno essere realizzati anche in collaborazione con altre istituzioni scolastiche.

8.3 Interventi formativi di aggiornamento

In sede di verifica dell'efficacia delle misure di sicurezza, anche in relazione a novità che di dovessero presentare nelle norme di legge e/o in relazione all'evoluzione tecnica del settore, il titolare ed il responsabile programmeranno le necessarie attività formative.

Le attività formative sui contenuti di cui si tratta verranno certificate ed annotate su un apposito registro.

9 - MISURE SPECIFICHE PER I DATI PERSONALI IDONEI A RIVELARE LO STATO DI SALUTE

Questa istituzione tratta dati idonei a rivelare lo stato di salute del personale, docente ed ATA, e degli alunni esclusivamente per finalità previste dalla legge.
Secondo quanto prescritto dall'articolo 22 comma 7 del D. lgs 196/2003 i dati idonei a rivelare lo stato di salute *"sono conservati separatamente da altri dati personali trattati per finalità che non richiedono il loro utilizzo";* inoltre il comma 7 dello stesso articolo dispone che i dati idonei a rivelare lo stato di salute, qualora contenuti in banche dati

informatiche vengano trattati *"con tecniche di cifratura o mediante l'utilizzo di codici identificativi o di altre soluzioni, che li rendono temporaneamente inintellegibili anche a chi è autorizzato ad accedervi e permettono di identificare gli interessati solo in caso di necessità".*

Riguardo al trattamento senza l'ausilio di strumenti elettronici, dei dati di cui si tratta si stabilisce quanto segue:

a) Dati riguardanti il personale docente ed ata

I dati consistono essenzialmente in certificati medici consegnati o fatti pervenire all'ufficio di segreteria.
Dopo la ricezione, durante il trattamento (protocollazione etc) saranno inseriti in una contenitore chiuso riferito all'interessato e successivamente inseriti nel fascicolo personale, dove saranno conservati all'interno di una busta chiusa recante l'indicazione del contenuto separatamente dagli altri documenti.

b) Dati riguardanti gli alunni

I dati consistono essenzialmente in certificati medici consegnati dagli alunni o dai genitori ai docenti o al personale ATA, per scopi definiti da norme di legge (giustificazione assenze; esonero da attività di educazione fisica, necessità di particolari diete alimentari etc.)
Dopo la ricezione i dati saranno inseriti in una contenitore chiuso riferito all'interessato e successivamente trattati da personale incaricato e custoditi in appositi contenitori chiusi.
I certificati riguardanti la necessità di particolari diete alimentari, potranno in caso di necessità, essere comunicati al soggetto che espleta il servizio mensa previamente nominato responsabile esterno del trattamento da parte del titolare.

10 - FORMALIZZAZIONE DEL DOCUMENTO

Il presente documento verrà posto all'approvazione del Consiglio di Istituto o/e Collegio Docenti.
Verrà in seguito emanato un Regolamento interno per la Sicurezza dei Dati che si baserà su quanto analizzato in questo Documento.

Viterbo, 19/03/11

Il **Titolare del Trattamento** : Prof.ssa Paola Moscucci

Data 19/03/11 Firma _____

Il Responsabile del Trattamento: Sig.ra SCALZINI MARIA TERESA

Data 19/03/11 Firma _____