



MINISTERO DELLA PUBBLICA ISTRUZIONE
ISTITUTO COMPRENSIVO STATALE "A. STROBINO"
VIA BOCCACCIO N. 2 – CERRO MAGGIORE - MI

Il Dirigente scolastico

Visto il decreto legislativo 30 giugno 2003, n.196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 33 e ss., nonché l'allegato B del suddetto D.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza;

Considerato che l'istituto comprensivo statale "A. Strobino" è titolare del trattamento di dati personali ai sensi dell'art.28 del d.lgs. n. 196 del 2003;

Visto l'obbligo di prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del D.lgs. n.196 del 2003;

Visto il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, emanato con Decreto Ministeriale n.305 del 7.12.2006;

Adotta il DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento, elaborato al fine di mettere in atto le misure di sicurezza per tutelare i dati personali oggetto di trattamento, fornisce una individuazione dei criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati a misure di sicurezza e dei criteri per assicurare l'integrità dei dati, da adottare per il trattamento dei dati personali effettuato dal personale dell'istituto comprensivo statale "A. Strobino" il cui legale rappresentante pro-tempore è il dirigente scolastico dr. Anna Mennilli che nel seguito del documento sarà indicato come "titolare". Il presente documento è aggiornato periodicamente ed i termini utilizzati seguono le definizioni riportate all'art.4 del D.lgs 196/2003. Del documento fanno parte integrante le schede allegate al Regolamento del Ministero della Pubblica Istruzione citato nelle premesse.

1 Elenco dei trattamenti di dati personali

1.1 Finalità

Il trattamento dei dati personali è funzionale al raggiungimento delle finalità di istruzione e di formazione in ambito scolastico, professionale e superiore, con particolare riferimento a quelle svolte anche in forma integrata, ed è quindi di rilevante interesse pubblico, ai sensi degli articoli 20 e 21 del D.lgs 196/2003. Per le sue finalità istituzionali, l'Istituzione scolastica tratta dati personali, sia comuni che sensibili o giudiziari, di studenti, genitori, personale dipendente e fornitori.

1.2 Luoghi di tenuta e trattamento dei dati:

I dati su supporto cartaceo sono conservati negli armadi degli uffici amministrativi: del personale, didattica alunni e protocollo, ufficio contabilità e nel corridoio adiacente tali Uffici, stanza denominata archivio storico, nell'Ufficio del dirigente. nell'Ufficio del collaboratore vicario.

I dati acquisiti attraverso il protocollo riservato sono conservati nell'ufficio del dirigente scolastico.

I dati su supporto elettronico sono conservati negli archivi elettronici del server e alcuni su computer di tutti i servizi amministrativi.

(Nella tabella che segue, relativamente ai dati sensibili e giudiziari, nella descrizione sintetica del trattamento, le finalità e le attività svolte, i tipi di dati trattati e le operazioni eseguite sono indicati in modo sintetico e con riferimento alle schede allegate al Regolamento del Ministero della Pubblica Istruzione citato nelle premesse, con specificazione, per ogni identificativo di trattamento, delle specifiche schede)

Tabella 1.1 – Elenco dei trattamenti: informazioni essenziali (regola 19.1 del disciplinare tecnico)

<i>Id Trattamento</i>	<i>Descrizione sintetica del trattamento</i>			<i>Natura dei dati</i>		<i>Struttura di riferimento</i>	<i>Altre strutture che concorrono al trattamento</i>
	<i>Finalità perseguita o attività svolta</i>	<i>Categorie di interessati</i>	<i>Terzi a cui vengono comunicati i dati</i>	<i>S</i>	<i>G</i>		
T1	Gestione Area Alunni Relativamente ai dati sensibili e giudiziari : Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico; Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	Alunni Genitori	USP, MPI, Altre istituzioni scolastiche, AUSL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, , Avvocature dello Stato, Magistrature ordinarie e amministrativo-contabile, Organi di polizia giudiziaria, Liberi professionisti	S	S	A2.2	A5 – A3.1 – A7
T2	Gestione Area Bilancio	Personale Fornitori	USP, USP, MPI, Agenzia delle Entrate, Altre istituzioni scolastiche, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Banca che effettua il servizio di cassa			A3.2	

T3	Gestione Area Personale Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e reclutamento a TI e TD 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. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	Personale	USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego, Centro per l'impiego della Provincia di Milano	S	S	A1.1	A1.2 – A2.3 – A3.2
T4	Gestione Area Retribuzioni Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro; Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari; Scheda n. 3 – Organismi collegiali e commissioni istituzionali;	Personale	USP, USR, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Magistrature ordinarie e amministrativo-contabile, Agenzia delle Entrate, Banca che effettua il servizio di cassa, Centro per l'impiego della Provincia di Milano	S	S	A1.2	A3.2

T5	Gestione Fiscale	Personale	USP, MPI, Agenzia delle Entrate, Corte dei Conti, Enti assistenziali, previdenziali e assicurativi, MEF, Banca che effettua il servizio di cassa			A1.2	A3.2
T6	Gestione Protocollo Relativamente ai dati sensibili e giudiziari: Tutte le schede allegare al regolamento sul trattamento dei dati sensibili e giudiziari	Alunni, Genitori, Fornitori, Personale, Altre amministrazioni	USP, USP, MPI, Altre istituzioni scolastiche, Ordinario Diocesano, Organizzazioni Sindacali, Presidenza del Consiglio, INPDAP, INPS, INAIL, AUSL, Altre Amministrazioni Pubbliche, Corte dei Conti, MEF, Enti assistenziali, previdenziali e assicurativi, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Agenzia delle Entrate, Organi preposti agli accertamenti idoneità impiego, Banca che effettua il servizio di cassa	S	S	A1.3	
T7	Gestione Sicurezza	Personale amministrativo accesso aree Sissi				-A4	A3.2
T8	Backup e Restore	Banca dati Sissi Amministrativa Server				A4	A3.2
T9	Gestione Protocollo e corrispondenza riservata Relativamente ai dati sensibili e giudiziari: Tutte le schede allegare al regolamento sul trattamento dei dati sensibili e giudiziari	Alunni, genitori, personale	USP, MPI, Altre istituzioni scolastiche, AUSL, Enti Locali, Gestori pubblici e privati dei servizi di assistenza, Istituti di assicurazione, INAIL, Aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola lavoro, Avvocature dello Stato, Magistrature ordinarie e amministrativo-contabile, Organi preposti alla vigilanza su igiene e sicurezza, Autorità di pubblica Sicurezza, Organi di polizia giudiziaria, Liberi professionisti	S	S	A3.1	

T10	Gestione della posta elettronica	Personale, utenti del servizio scolastico, fornitori				A1.1	A1.3
T11	Gestione Scioperi del Personale dipendente Relativamente ai dati sensibili e giudiziari : Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;	Personale	https://websptnet.tesoro.it/SCI OPNET	S		A1.1	A1.3
T12	Gestione Anagrafe delle prestazioni	Personale interno ed esterno, Fornitori	www.anagrafeprestazioni.it				
T13	Invio documenti tramite Entratel e DMA	Personale esterno e della scuola	Sito entratel			A1.2	A3.2
T14	Gestione Pre96	Personale interno alla scuola	Ragioneria Provinciale del Tesoro			A1.2	A3.2
T15	Gestione INPS DM10 - EMENS	Personale interno alla scuola	INPS	S		A1.2	A3.2
T16	Gestione Microsoft Office comunicazione	Personale interno ed esterno, Fornitori				Tutte	Tutte
T17	Gestione Dispositivi dell'infrastruttura tecnologica	Personale interno ed esterno, Fornitori				A4	

T18	Gestione Provvedimenti Disciplinari alunni Relativamente ai dati sensibili e giudiziari : Scheda n. 4 – Attività propedeutiche all’avvio dell’anno scolastico; Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione; Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.	Genitori, Alunni, Personale	Genitori, USP	S		A3.3	A1.3
T19	Gestione Graduatorie e supplenze	Personale	USP, USR, MPI			A1.1	A1.3
T20	Gestione del personale	Personale		S	S	A1.1	A1.3 – A3.2
T21	Gestione Contratti con esperti esterni	Personale interno ed esterno	Enti Pubblici Territoriali, INPS, , AGENZIA ENTRATE FISCALI ANAGRAFE PRESTAZIONI, INAIL, Organizzazioni Sindacali, Ditte Esterne			A1.4	A1.3 – A1.2
T22	Gestione Trattative sindacali Relativamente ai dati sensibili e giudiziari : Scheda n. 3 – Organismi collegiali e commissioni istituzionali;	Contrattazione sindacale	Componenti RSU Organizzazioni Sindacali	S		A3.1	A1.3
T23	Gestione Archivio cartaceo storico	Tutte le categorie	I dati non vengono comunicati a terzi (prima dell’eventuale comunicazione vengono trasferiti alle strutture interne autorizzate al trattamento)	S	S	A5	
T24	Gestione Assistenza e manutenzione hardware	Tutti i soggetti che utilizzano i PC degli uffici Amministrativi				A4	

T25	Gestione titolare Generale		USP, USR, MPI			A1.3	
T26	Gestione Riproduzione e notifica documenti	Personale, Alunni, Genitori Fornitori				A7	
T27	Gestione Atti cartacei amministrativi	Personale, Alunni, Genitori Fornitori				A6	
T28	Gestione Inventario e Fornitori di beni e servizi	Ditte esterne	Ditte esterne			A2.1	A3.1

Tabella 1.2 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti (regola 19.1 del disciplinare tecnico)

<i>Id Trattamento</i>	<i>Applicativo</i>	<i>Banca Dati</i>	<i>Ubicazione fisica dei supporti di memorizzazione</i>		<i>Tipologia dei dispositivi di accesso</i>	<i>Tipologia di interconnessione</i>
			<i>Luogo</i>	<i>Elaboratore</i>		
T1	<i>Software gestionale SISSI</i>	Serversissi	Armadio Rec server Corridoio Uffici	SERVER	PC	Internet - Intranet
T2	<i>Software gestionale SISSI</i>	Serversissi	Armadio Rec server Corridoio Uffici	SERVER	PC	Internet - Intranet
T3	<i>Software gestionale SISSI</i>	Serversissi	Armadio Rec server Corridoio Uffici	SERVER	PC	Internet - Intranet
T4	<i>Software gestionale SISSI</i>	Serversissi	Armadio Rec server Corridoio Uffici	SERVER	PC	Internet - Intranet
T5	<i>Software gestionale SISSI</i>	Serversissi	Armadio Rec server Corridoio Uffici	SERVER	PC	Internet - Intranet
T6	<i>Software gestionale SISSI</i>	Serversissi	Armadio Rec server Corridoio Uffici	SERVER	PC	Internet - Intranet
T7	<i>Software gestionale SISSI</i>	Serversissi	Armadio Rec server Corridoio Uffici	SERVER	PC	Internet - Intranet
T8	<i>Software gestionale SISSI</i>	Serversissi	Armadio Rec server Corridoio Uffici	SERVER	PC	Internet - Intranet
T9	Microsoft Office	PC Dirigente scolastico	Stanza Dirigente Scolastico	PC Dirigente	PC	Intranet

T10	Outlook Express – Area Riservata Ministero Istruzione	Pc Ufficio Protocollo	Didattica	PC PROTOCOLLO	PC	Internet - Intranet
T11	Accesso area riservata Min. Tesoro	Ministero Tesoro	PERSONALE	N. 2 PC PERSONALE	PC	
T12	Sito Anagrafe delle Prestazioni	Ministero Istruzione	CONTABILITA'	N. 1 PC CONTABILITA'	PC	
T13	Sito riservato Agenzia Entrate ENTRATEL	Agenzia Entrate	UFFICIO D.S.G.A.	N. 1 PC. DSGA	PC	
T14	Sito riservato PROVINCIA DI MILANO	PROV. Milano	PERSONALE	n. 2 P.C. PERSONALE	PC	
T15						
T16	Microsoft Office	Pc Ufficio	Tutti gli uffici	Tutti gli Uffici	PC	Intranet
T17						
T18	Microsoft Office	Pc Ufficio collaboratore Dirigente Scolastico				
T19	Accesso Area Riservata Ministero Istruzione	PC Ufficio Personale	PC Ufficio Personale	PC Ufficio Personale		Intranet
T20	Applicativo Sissi	Serversissi	Serversissi	Serversissi		Intranet
T21	Microsoft Office	Pc Ufficio	Pc Ufficio Protocollo	Pc Ufficio Protocollo		Intranet
T22	Microsoft Office	PC Dirigente scolastico	PC Dirigente scolastico	PC Dirigente Scolastico		Intranet
T23	Contenitori per archivio	Archivio storico	Archivio storico	Archivio storico		
T24						
T25						
T26						
T27						

T28						
------------	--	--	--	--	--	--

Tabella 1.3 – Elenco dei trattamenti: ulteriori elementi per descrivere gli strumenti cartacei (regola 19.1 del disciplinare tecnico)

<i>Id Trattamento</i>	<i>Archivio cartaceo</i>	<i>Ubicazione logistica</i>		
			<i>Stanza</i>	<i>Armadio</i>
T23	Raccoglitori cartacei	Scaffalatura con raccoglitori specifici e numerati dell'ufficio	Archivio storico	
T27	Armadi e scaffali metallici	Scaffalatura con raccoglitori specifici e numerati dell'ufficio	Ufficio di competenza	

2 Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati

Le misure indicate nel presente documento sono relative alla sede centrale dell'istituzione scolastica.

Le procedure di trattamento dei dati avvengono nella sola sede centrale, considerato che i dati oggetto delle misure indicate nel presente documento sono trattenuti presso le altre sedi solo per il tempo necessario a provvedere all'inoltro alla sede centrale. I dati sono trattenuti sotto la responsabilità degli incaricati (docenti e responsabile della sede) in cassetto chiuso del quale detengono la chiave. L'inoltro avviene in busta chiusa per il tramite del personale della scuola con consegna all'ufficio protocollo.

Il titolare del trattamento ha designato, ai sensi dell'art.29 D.lgs 196/2003, con atto scritto contenente analitiche istruzioni relative ai compiti affidati, il responsabile del trattamento nella persona del DSGA sig. Renato Lovisolo.

Il responsabile del trattamento ha provveduto, sulla base della lettera di designazione e delle disposizioni dell'art.30, ad individuare gli incaricati del trattamento dei dati personali appartenenti ai profili professionali del personale ATA; ha conferito agli stessi l'incarico con atto scritto contenente puntuali istruzioni relative agli ambiti di trattamento consentiti, corredato da linee guida e con allegate le schede relative al trattamento dei dati sensibili e giudiziari.

Il Responsabile del trattamento ha provveduto altresì a individuare, nominare e incaricare per iscritto un incaricato della gestione e della manutenzione degli strumenti elettronici, un incaricato della custodia delle copie delle credenziali e un incaricato delle copie di sicurezza delle banche dati ai quali sono state fornite puntuali istruzioni relative ai compiti da svolgere. Il titolare ha direttamente provveduto ad individuare e incaricare il personale docente con atto che fornisce le istruzioni necessarie. I singoli incaricati, che hanno rilasciato ricevuta della avvenuta consegna della lettera di incarico, sono stati informati che l'ambito dei trattamenti autorizzati è suscettibile di aggiornamento periodico e che sono tenuti ad attenersi al divieto di comunicazione e diffusione dei dati trattati nel corso dell'incarico, anche per il tempo successivo alla sua cessazione, senza limiti temporali.

La comunicazione dei soggetti previsti dal D.lgs 196/2003 è avvenuta attraverso la pubblicazione all'albo della scuola dell'organigramma della scuola e delle responsabilità.

A tutti gli incaricati del trattamento di dati mediante strumento elettronico sono state conferite credenziali di autenticazioni (art.34, comma 1, lett.b) mediante parola chiave, conformi alle caratteristiche indicate nell'allegato B. Agli incaricati sono state fornite puntuali indicazioni per la modifica della parola chiave ogni tre mesi. La modifica della password è curata direttamente dagli incaricati oppure dal responsabile delle credenziali.

Tabella 2 – Competenze e responsabilità delle strutture preposte ai trattamenti (regola 19.2)

<i>Id Struttura</i>	<i>Struttura</i>	<i>Trattamenti effettuati</i>	<i>Descrizione dei compiti e delle responsabilità</i>
A1.1	Ufficio Personale	T3 – T10 – T11	<ul style="list-style-type: none"> • Uso applicativo Sissi – Protocollo in uscita • Gestione dei documenti office automation • Accesso all'area riservata del sito Istruzione • Accesso al servizio di gestione degli scioperi • Consultazione e archiviazione dei fascicoli personali dei dipendenti • Gestione del software per la rilevazione delle presenze del personale • Gestione della posta elettronica • Gestione delle comunicazione contratti on line alla Provincia di Milano
A1.2	Ufficio Contabilità	T2 – T13 –T14	<ul style="list-style-type: none"> • Uso applicativo Sissi Area contabilità – Protocollo in uscita • Gestione dei documenti office • Accesso all'area riservata del sito Istruzione • Gestione della documentazione cartacea relativa al bilancio • Invio Documenti Entratel • Invio documenti PRE96 • Invio DMA • Invio DM10 - EMENS
A1.3	Ufficio Protocollo	T6	<ul style="list-style-type: none"> • Uso applicativo Axios Area protocollo POSTA IN ENTRATA E IN USCITA • Gestione dei documenti office • Stampe registro protocollo • Smistamento e archiviazione corrispondenza
A1.4	Ufficio Contabilità	T12 –T21	<ul style="list-style-type: none"> • Gestione dei documenti office • Contratti personale esterno Istituzione scolastica • Tenuta registri contratti
A2.1	Ufficio Contabilità	T28	<ul style="list-style-type: none"> • Gestione dei documenti office automation • Tenuta Inventario beni • Rapporti con i fornitori • Gare e acquisti di beni e servizi

A2.2	Ufficio Didattica Alunni	1	<ul style="list-style-type: none"> • Utilizzo dell'applicativo Sissi Area Alunni • Gestione dei documenti di office • Accesso all'area riservata del sito www.istruzione.it • Utilizzo applicativo GIS per produzione denunce di infortunio • Consultazione e archiviazione dei fascicoli personali degli alunni • Rilevazione assenze alunni della scuola
A3.1 A3.3	Ufficio Dirigente Scolastico Ufficio Collaboratore del D.S.	T22 -T9 - T18	<ul style="list-style-type: none"> • Gestione degli Organi collegiali • Gestione dell'offerta formativa • Gestione della sicurezza sul posto di lavoro legge 626 • Gestione della protezione dei dati personali • Relazioni sindacali • Rapporti con gli enti • Gestione Protocollo Riservato • Gestione Provvedimenti disciplinari alunni • •
A3.2	Ufficio Direttore Servizi Generali e Amministrativi	T1-T2-T3-T4-T5-T6-T7	<ul style="list-style-type: none"> • Gestione del Bilancio • Utilizzo di tutti gli applicativi Sissi • Gestione rapporti con il personale • Organizzazione del Lavoro ATA • Concessione credenziali accesso aree riservate
A4	Amministratore di Sistema	T8 - T17 -T24	<ul style="list-style-type: none"> • Amministra il Server di sistema sissi con il Dbase SISSI • Amministra i sistemi operativi dei clients in rete • Amministra e configura il router per l'accesso ad internet • Provvede agli aggiornamenti degli applicativi Sissi e la loro installazione • Predisporre l'automazione del backup dell'archivio SISSI • Installa sui client della rete amministrativa idoneo Antivirus • Installa su tutte le macchine idonei programmi antispywere
A5	Personale Docente	T1	<ul style="list-style-type: none"> • Trattamento dati degli alunni
A6	Archivio storico	T23 - T27	<ul style="list-style-type: none"> • Gestione e archiviazione Atti Amministrativi dell'Istituzione Scolastica
A7	Personale Ausiliario	T26	<ul style="list-style-type: none"> • Riproduzione mediante fotocopiatura dei documenti e notifica degli stessi • Rilevazione presenze mensa alunni - Diete speciali • Distribuzione registri di classe all'inizio delle lezioni e raccolta degli stessi al termine.

3 Analisi dei rischi che incombono sui dati

La ricognizione e l'analisi dei rischi, che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuita, in grado di recare pregiudizio ai dati personali trattati, è stata riportata nelle tabelle che seguono nelle quali gli eventi sono stati suddivisi in tre categorie:

1) Comportamenti degli operatori.

Sottrazione di credenziali di autenticazione; carenza di consapevolezza, disattenzione o incuria; comportamenti sleali o fraudolenti; errori materiali.

2) Eventi relativi agli strumenti.

Danno arrecato da virus informatici o di programmi suscettibili di recare danno; spamming o tecniche di sabotaggio; malfunzionamento, indisponibilità o usura degli strumenti; accessi esterni non autorizzati; intercettazione di informazioni in rete.

3) Eventi relativi al contesto fisico-ambientale.

Accessi non autorizzati a locali ad accesso ristretto; eventi distruttivi naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc) nonché dolosi, accidentali o dovuti ad incuria; guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc); errori umani nella gestione della sicurezza fisica.

I suddetti rischi sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione, adottando la seguente scansione:

Alta - Bassa - Molto Elevata - Media - Medio-Alta - Medio-Bassa

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

Tabella 3 – Analisi dei rischi (regola 19.3 del disciplinare tecnico)

	<i>Id Rischio</i>	<i>Rischi</i>	<i>Si/No</i>	<i>Descrizione dell'impatto sulla sicurezza (gravità:alta/media/bassa)</i>
Comportamento degli operatori	R1	Sottrazione di credenziali di autenticazione.	Si	Alta
	R2	Carenza di consapevolezza, disattenzione o incuria.	Si	Media
	R3	Comportamenti sleali o fraudolenti.	Si	Bassa
	R4	Errore materiale.	Si	Media
Eventi	R5	Azione di <i>virus</i> informatici o di programmi suscettibili di recare danno.	Si	Alta

	R6	Spamming o tecniche di sabotaggio.	Si	Alta
	R7	Malfunzionamento, indisponibilità o degrado degli strumenti.	Si	Media
	R8	Accessi esterni non autorizzati.	Si	Media
	R9	Intercettazione di informazioni in rete.	Si	Media
contesto	R10	Accessi non autorizzati a locali/reparti ad accesso ristretto.	Si	Bassa
	R11	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc,) nonché dolosi, accidentali o dovuti ad incuria.	Si	Media
	R12	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, ecc.).	Si	Media
	R13	Errori umani nella gestione della sicurezza fisica.	Si	Media

4 Misure da adottare per garantire l'integrità e la disponibilità dei dati, non che la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità

Contro i rischi d'intrusione i locali della sede centrale, unica sede nella quale sono detenuti dati soggetti a protezione, sono dotati di impianto d'allarme a sensori infrarossi, attivabile mediante digitazione d'un codice consegnato al personale collaboratore scolastico dipendente, al dirigente scolastico, al direttore amministrativo. La gestione dell'impianto di allarme antifurto, così come l'attribuzione dei codici, è curata dal Comune di Cerro Maggiore Ufficio Vigilanza. E' stata disposta l'attivazione dell'allarme al termine dell'orario di lavoro.

Per garantire la sicurezza delle aree in cui i dati sono trattati elettronicamente, sono state introdotte sui personal computer password di BIOS, e password di rete, trimestralmente cambiate.

Le aree contenenti dati in supporto cartaceo (archivio e mobili contenenti documentazione contabili dei dipendenti e degli alunni) sono ubicate in modo tale che ciascun addetto possa rilevare a vista e impedire il tentativo di accesso da parte di persone estranee.

Sono state impartite disposizioni affinché, in assenza del personale, le stanze rimangano chiuse e le chiavi siano custodite dal personale collaboratore scolastico in servizio addetto alla vigilanza che, al termine del servizio, provvederà al deposito delle chiavi nell'apposito contenitore.

L'ubicazione di stampanti ed apparecchio telefax tradizionale non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale.

Di seguito si illustrano le norme applicate per garantire la sicurezza e l'integrità dei dati per:

- *Computer e supporti informatici*: Il server è collegato ad un gruppo di continuità che consente di escludere la perdita di dati derivanti da sbalzi di tensione o di interruzione di corrente elettrica. L'integrità dei dati sul server amministrativo è garantita da una tripla procedura di backup: la prima avviene in automatico con apposito software che giornalmente opera il salvataggio di una copia del data base Sissi sul server stesso; la seconda è effettuata normalmente masterizzando su CD ROM ogni venerdì pomeriggio, la terza settimanalmente è eseguita mediante unita dat salvando oltre al db c:\sissi\sys\bck\tmp anche i documenti di tutte le postazioni alloggiate sul server, i backup di tutta la settimana sono eseguiti sul server. I CD ROM vengono conservati per almeno due mesi nell'apposta cassaforte. Il server della rete amministrativa viene protetto da password per impedire al personale non autorizzato l'accesso alla rete amministrativa. Le password sono assegnate e riportate su un apposito foglio conservato nella cassaforte collocata nella stanza del DSGA. L'introduzione di password di BIOS all'accensione dei personal computer, di password dello screen-saver e di password per l'accesso in rete determina un soddisfacente livello di protezione dei dati contenuti nei PC. L'introduzione delle password e di apposito software antivirus inibisce ad estranei l'uso dei personal computer, attraverso i quali, tramite Proxy, si accede alla posta elettronica.
- Il Server viene acceso all'inizio del turno di lavoro antimeridiano dagli assistenti amministrativi e viene spento al termine del turno di lavoro dagli assistenti amministrativi o dal dsga in servizio nel turno pomeridiano.
- Per l'invio di messaggi e-mail a più destinatari, sono state fornite al personale istruzioni affinché quale destinatario venga sempre indicata la scuola con l'indirizzo e-mail e in CCN i destinatari, in modo che non possano essere individuati gli indirizzi e-mail degli altri destinatari attraverso la funzione di proprietà.
I CD ROM masterizzati e le cassette dat contenenti copie degli archivi sono custoditi negli appositi contenitori di plastica e inseriti nella armadietto blindato ubicato all'interno dell'armadio principale blindati entrambi sono sempre chiusi con serratura meccanica. I floppy disk contenenti dati degli studenti, delle famiglie degli stessi, dei lavoratori dipendenti e collaboratori, possono essere riutilizzati esclusivamente dopo opportuna formattazione, in modo da impedire la lettura dei dati precedenti, così come stabilito dalla legge. I CD ROM non più utilizzabili vengono distrutti.
I floppy disk contenenti dati, prima della formattazione, sono custoditi nello stesso modo dei CD e delle cassette DAT contenenti copie degli archivi. Per quanto riguarda infine l'obbligo previsto dalle misure minime sulla sicurezza di cui all'allegato B del codice della privacy, i computer sono dotati di programma antivirus che è aggiornato sotto la responsabilità del titolare del trattamento a cadenza almeno trimestrale e che consente di rilevare immediatamente all'apertura di un file la presenza di un virus.
- *Supporti cartacei*: relativamente ai supporti cartacei sono state impartite dettagliate istruzioni a tutto il personale al momento dell'affidamento dell'incarico e nel corso degli interventi di formazione. (vedi lettere di individuazione degli incaricati del trattamento dei dati e Linee Guida allegate)
- *Gestione della privacy e trattamento dei dati raccolti attraverso il sito Web*

Tabella 4.1 – Le misure di sicurezza adottate o da adottare (regola 19.4 del disciplinare tecnico)

<i>Id Misura</i>	<i>Misura</i>	<i>Descrizione e dei rischi contrastati</i>	<i>Trattamenti interessati</i>	<i>Misura già in essere</i>	<i>Misura da adottare</i>	<i>Struttura o persone addette all'adozione</i>
M1	Predisposizione dei profili di autorizzazione di accesso agli applicativi Sissi	R1,R2,R3, R4	T7	X		A4 – Amministratore di Sistema
M2	Procedura formale di concessione delle credenziali per l'utilizzo degli applicativi Sissi	R1,R2,R3, R4	T7	X		A4 – Amministratore di Sistema

M3	Procedura per la concessione di credenziali per l'accesso all'area riservata di Istruzione.it	R1,R2,R3, R4	T7	X		A3.2 – Ufficio DSGA
M4	Concessione delle credenziali per l'accesso a SIMPI	R1,R2,R3, R4	T7	X		A3.2 – Ufficio DSGA
M5	Concessione credenziali per la gestione della posta elettronica	R1,R2,R3, R4	T10	X		A3.2 – Ufficio DSGA
M6	Concessione delle credenziali per l'accesso all'applicativo per le denunce di infortunio alunni	R1,R2,R3, R4	T1	X		A3.2 – Ufficio DSGA
M7	Concessione credenziali accesso sito rilevazione scioperi	R1,R2,R3, R4	T11	X		A3.2 – Ufficio DSGA
M8	Concessione delle credenziali per l'accesso al sito Anagrafe Prestazioni	R1,R2,R3, R4	T14	X		A3.2 – Ufficio DSGA
M9	Concessione delle credenziali per l'accesso al sito Entratel	R1,R2,R3, R4	T13	X		A3.2 – Ufficio DSGA
M10	Concessione delle credenziali per l'accesso alla spedizione telematica del DM10	R1,R2,R3, R4	T13	X		A3.2 – Ufficio DSGA
M11	Concessione delle credenziali per l'accesso al servizio di invio de conguaglio fiscale	R1,R2,R3, R4	T13	X		A3.2 – Ufficio DSGA
M12	Concessione delle credenziali per l'accesso ai dispositivi di amministrazione del sistema informativo	R1,R2,R3, R4, R8,R9	T4	X		A4 – Ufficio DSGA
M13	Concessione delle credenziali per l'accesso di ciascun utente del sistema alle risorse del dominio locale	R1,R2,R3, R4	T7	X		A4 – Ufficio DSGA
M14	Installazione Antivirus sui PC della rete Amministrativa	R5,R6	T7	X		A4 – Ufficio DSGA
M15	Redazione di un disciplinare tecnico per le procedure di Backup con cadenza almeno settimanale	R5,R7,R11, R12,R13	T7	X		A4 – Ufficio DSGA
M16	Verifica delle procedure di ripristino di Backup	R5,R7,R11, R12,R13	T7	X		A4 – Ufficio DSGA
M17	Configurazione o ripristino del sistema operativo dei clients	R1,R2,R3, R4	T7	X		A4 – Ufficio DSGA
M18	Redazione di un disciplinare tecnico per la conservazione dei supporti di memorizzazione removibili	R5,R7,R11, R12,R13	T7	X		A4 – Ufficio DSGA

M19	Predisposizione di un piano di interventi di manutenzione dell'Hardware al fine di garantire l'integrità dei dati	R7	T7	X		A4 – Ufficio DSGA
M20	Procedura di concessione delle autorizzazioni all'accesso dei documenti cartacei	R10,R13	T27	X		A3.2 – Ufficio DSGA
M21	Impianto del registro degli accessi ai locali dell'ufficio dopo l'orario di chiusura	R10,R13	T27	X		A3.2 – Ufficio DSGA
M22	Installazione nei locali in cui sono contenuti gli archivi informatici e cartacei di un impianto antifurto	R10,R13	T24	X		A4 – Ente Locale
M23	Predisposizione di armadi provvisti di chiusura per la custodia dei documenti	R10,R13	T24	X		A4 – Ufficio Dsga
M24	Procedura formale di consegna delle chiavi degli armadi agli incaricati dei trattamenti	R10,R13	T7	X		A3.2 – Ufficio DSGA
M25	Procedura formale di concessione delle autorizzazioni per l'accesso ai locali	R10,R13	T7	X		A3.2 – Ufficio DSGA

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°1		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M1				
Descrizione sintetica	Predisposizione dei profili di autorizzazione di accesso agli applicativi Sissi				
Elementi Descrittivi	Tramite il programma di gestione sicurezza di Sissi , assegnazione all'utente identificato dal DSGA di nome utente e password per l'accesso al software specifico di lavoro. Con opzioni di Visualizzazione e Modifica oppure solo Visualizzazione dei dati L'accesso al software SICUREZZA SISSI è consentito all'amministratore di sistema.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°2		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M2				
Descrizione sintetica	Procedura formale di concessione delle credenziali per l'utilizzo degli applicativi sissi				
Elementi Descrittivi	Comunicazione da parte del DSGA del nome dell'utente e dell'applicativo che andrà ad utilizzare. Scelta della password usata per l'accesso. La password viene comunicata all'utente in busta chiusa con il nome utente utilizzato per l'accesso. L'elenco completo delle password è custodito in apposita cassaforte accessibile tramite chiavi meccaniche.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°3		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M3				
Descrizione sintetica	Procedura per la concessione di credenziali per l'accesso all'area riservata di Istruzione.it				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				

Data di aggiornamento	15 marzo 2007	
------------------------------	---------------	--

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°4		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M4				
Descrizione sintetica	Concessione delle credenziali per l'accesso a SIMPI				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°5		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M5				
Descrizione sintetica	Concessione credenziali per la gestione della posta elettronica				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				

Data di aggiornamento	15 marzo 2007	
------------------------------	---------------	--

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°6		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M6				
Descrizione sintetica	Concessione delle credenziali per l'accesso all'applicativo per le denunce di infortunio				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°7		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M7				
Descrizione sintetica	Concessione credenziali accesso sito rilevazione scioperi				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°8		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M8				
Descrizione sintetica	Concessione delle credenziali per l'accesso al sito Anagrafe Prestazioni				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°9		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M9				
Descrizione sintetica	Concessione delle credenziali per l'accesso al sito Entratel				
Elementi Descrittivi	Le credenziali per l'accesso al sito ENTRATEL vengono concesse dal servizio ministeriale dell'Agenzia delle Entrate. Il DSGA individuato l'operatore consegna le credenziali di accesso.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°10		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M10				
Descrizione sintetica	Concessione delle credenziali per l'accesso alla spedizione telematica del DM10				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°11		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M11				
Descrizione sintetica	Concessione delle credenziali per l'accesso al servizio di invio del conguaglio fiscale				
Elementi Descrittivi	Le credenziali per l'accesso al servizio vengono rilasciate al DSGA dagli uffici competenti, il quale delega il personale preposto al tipo di servizio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°12		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
--------------------	--	--------------------------	--	--	------------------

Misura	M12	
Descrizione sintetica	Concessione delle credenziali per l'accesso ai dispositivi di amministrazione del sistema informativo	
Elementi Descrittivi	Il Dirigente scolastico e il DSGA individua tra il personale interno, in possesso delle relative competenze informatiche, la persona che amministra il sistema. La persona che amministra il sistema può avvalersi della consulenza di tecnici esterni che verranno di volta in volta individuati.	
Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°13		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M13				
Descrizione sintetica	Concessione delle credenziali per l'accesso di ciascun utente del sistema alle risorse del dominio				
Elementi Descrittivi	E' stato creato un profilo comune di rete generico. Le credenziali concesse sono tali da non recare nessun tipo di accesso deleterio per i dati archiviati.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°14		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M14				

Descrizione sintetica	Installazione Antivirus sui PC della rete Amministrativa	
Elementi Descrittivi	Il software antivirus è installato singolarmente sui clients. L'aggiornamento dell'antivirus viene effettuato in automatico via internet.	
Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°15		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M15				
Descrizione sintetica	Redazione di un disciplinare tecnico per le procedure di Backup con cadenza almeno settimanale				
Elementi Descrittivi	Il Backup del database viene effettuato in automatico da un apposito software installato sul server di rete, lo stesso effettua anche il ripristino del database. La copia del bck viene archiviata in una cartella di sistema del server. La cadenza del bck è giornaliera, un' ulteriore copia del bck viene effettuata ogni sette giorni su supporto magnetico "cassetta dat" e su supporto ottico dvd/cd quest'ultimo viene conservato per due mesi nell'apposito armadio blindato in dotazione in dotazione, mentre la cassetta dat viene riutilizzata per il successivo salvataggio la settimana successiva.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°16		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M16				

Descrizione sintetica	Verifica delle procedure di ripristino di Backup	
Elementi Descrittivi	Ogni due mesi, si provvede a testare il ripristino dei dati mediante restore del database sissi su un altro pc dove è installato il software necessario al termine della prova il db base installato su tale PC viene cancellato	
Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°17		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M17				
Descrizione sintetica	Configurazione o ripristino del sistema operativo dei clients				
Elementi Descrittivi	Ogni clients è fornito all'origine di disco di ripristino del sistema operativo. In caso di danneggiamento del sistema un tecnico allo scopo individuato verrà incaricato con apposito provvedimento per reinstallare e riconfigurare le funzionalità dell'apparecchio.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°18		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M19				

Descrizione sintetica	Predisposizione di un piano di interventi di manutenzione dell'Hardware al fine di garantire l'integrità dei dati	
Elementi Descrittivi	La verifica del funzionamento hardware è fatta con cadenza annuale. Le verifiche vengono effettuate sul server di rete SISSI. Sul server SISSI è installato il data base generale dei dati sia didattici che sensibili. La verifica principale consiste nel testare l'efficienza dei lettori cd-rom e l'integrità del Hard-disk.	
Data di aggiornamento	15 marzo 2007	

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°19		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M20				
Descrizione sintetica	Procedura di concessione delle autorizzazioni all'accesso dei documenti cartacei				
Elementi Descrittivi	Il DSGA individua, in base ai compiti assegnati ad ogni assistente amministrativo, la concessione ad accedere ai relativi archivi cartacei. In ogni caso, considerate le piccole dimensioni e l'organico degli Uffici ogni assistente amministrativo è abilitato ad accedere agli archivi cartacei della scuola.				
Data di aggiornamento	15 marzo 2007				

Tabella 4.2 – Scheda descrittiva delle misure adottate

Scheda n°20		Compilata da DSGA		Data di compilazione (Modifica)	14 dicembre 2005
Misura	M23				

Descrizione sintetica	Predisposizione di armadi provvisti di chiusura per la custodia dei documenti	
Elementi Descrittivi	Ogni Assistente Amministrativo assegnato all'ufficio preposto e tenuto alla conservazione dei documenti negli appositi armadi provvisti di serratura con chiave. Al termine dell'orario di lavoro l'ultimo assistente che lascia l'Ufficio è tenuto a verificare che tutti gli armadi contenti documenti siano chiusi e le chiavi riposte nell'armadietto	
Data di aggiornamento	15 marzo 2007	

CONSIDERATO che l'unità amministrativa si compone di n° 7 assistenti amministrativi e n. 1 direttore dei servizi generali e amministrativi ripartiti nei seguenti Uffici:

Ufficio Personale n. 2 unità

Ufficio Contabilità n. 2 unità

Ufficio Didattica (alunni/genitori) e protocollo n. 3 unità

ogni assistente amministrativo è abilitato ad accedere a tutte le aree di lavoro dell'Ufficio a cui è stato assegnato, all'occorrenza in caso di assenza di tutti gli assistenti assegnati alla stessa Ufficio verranno autorizzati utenti di altri uffici ad accedere alle singole applicazioni sissi in modalità modifica e visualizza.

5 Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento

Al fine di garantire il ripristino dei dati in seguito a distruzione o danneggiamento, l'istituzione scolastica dispone di idonee procedure di salvataggio periodico (backup) che consistono nell'utilizzo dell'apposito software di backup del programma di gestione amministrativo il quale crea in automatico una copia compressa dei dati, archiviandoli in un'apposita cartella del server, e di un masterizzatore DVD che salva i dati anche su disco DVD registrabile, da utilizzarsi giornalmente al termine dell'orario lavorativo.

Tabella 5.1 – Criteri e procedure per il ripristino della disponibilità dei dati (regola 19.5 del disciplinare tecnico)

Ripristino		
Banca dati / archivio dati	Criteri e procedure per il salvataggio e il ripristino dei dati	Pianificazione delle prove di ripristino
DATABASE SISSI	Prova di Restore su altro PC con installato l'ambiente sissi al termine della prova cancellazione del db sissi	Quindicinale
Documenti di Office application	E' stata predisposta una attività pianificata sul pc dell'utente di una masterizzazione della cartella documenti	Quindicinale

Documenti Posta elettronica	E' stata predisposta una attività pianificata sul PC utilizzato per la posta elettronica di masterizzazione dei dati di posta	Quindicinale
------------------------------------	--	---------------------

Tabella 5.2 – Criteri e procedure per il salvataggio dei dati (regola 19.5 del disciplinare tecnico)

Salvataggio			
Banca dati	Criteri e procedure per il salvataggio	Luogo di custodia delle copie	Struttura o persona incaricata del salvataggio
Server Supporto Magnetico DVD	Software applicativo sissi Copia archivi su CD registrabile	Armadietto blindato inserito nell'armadio blindato principale	Amministratore di Sistema

6 Previsione di interventi formativi degli incaricati del trattamento

Gli interventi formativi sono programmati nell'ambito del piano di formazione e aggiornamento del personale, con cadenza annuale, per rendere gli incaricati del trattamento edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. Sono previste idonee attività di formazione in occasione di innovazioni e/o modifiche delle norme e in relazione allo sviluppo scientifico/tecnologico dei mezzi e dei sistemi di protezione.

La formazione è altresì programmata al momento dell'ingresso in servizio, in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali. L'incarico al trattamento dei dati contiene, oltre alle istruzioni date dal responsabile, anche le linee guida per il trattamento dei dati, le informazioni relative al significato dei termini e le schede allegate al Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione. Gli incaricati partecipano alla riunione annuale per la verifica e la revisione del documento programmatico per la sicurezza. Verrà valutata l'eventuale partecipazione del personale della scuola alle iniziative formative organizzate dall'USR del Lazio.

Tabella 6 – Pianificazione degli interventi formativi previsti (regola 19.6 del disciplinare tecnico)

Descrizione sintetica degli interventi formativi	Classi di incarico o tipologie di incaricati interessati	Tempi previsti
Attuazione delle norme sulla riservatezza dei dati personali – Acquisizione di competenze giuridiche e di organizzazione scolastica – Responsabilità dei docenti nel trattamento dei dati personali con riferimento al REGOLAMENTO sul trattamento dei dati sensibili e giudiziari	Docenti incaricati del trattamento dei dati personali	1 ore di attività di formazione in un incontro di 1 ora – a.s. 2006/07

Miglioramento dell'attuazione delle norme sulla riservatezza dei dati personali nella scuola	Personale ATA della scuola	2 ore di attività di formazione- a.s. 2006/07
--	----------------------------	---

7 Descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare

Dati personali sono gestiti dal sistema informativo del MPI che non ha ancora comunicato le misure adottate e alcun documento programmatico.

8 Individuazione dei criteri da adottare per la cifratura o per la separazione dei dati personali idonei a rivelare lo stato di salute e la vita sessuale (Regola 19.8 del disciplinare tecnico)

Pur non rientrando fra gli organismi tenuti alla attuazione del punto 24, l'istituzione scolastica ha messo in atto particolari misure di protezione nell'archiviazione dei dati personali idonei a rivelare lo stato di salute, conservandoli sempre in busta chiusa inserita all'interno del fascicolo personale.

9 Conclusioni

Il presente documento sarà tempestivamente aggiornato nel caso di sostituzione di attrezzature o di cambiamenti nella disposizione degli spazi di lavoro e, in ogni caso, entro il 31 marzo di ciascun anno.

Agli incaricati del trattamento è stata data informazione circa il contenuto del presente documento, attraverso la consegna di una copia, con rilascio di ricevuta dell'avvenuta consegna, nella quale si dà atto della comunicazione dell'obbligo di uniformarsi al documento. Il responsabile del trattamento è tenuto a vigilare sull'osservanza delle disposizioni stesse da parte degli incaricati e a emanare ulteriori disposizioni relative alla gestione della sicurezza dei dati.

Il presente documento è stato illustrato nel corso di apposite riunioni, tenute in orario di lavoro, alle quali hanno partecipato il Dirigente Scolastico, il responsabile del trattamento ed il personale ATA incaricato del trattamento, nel rispetto delle disposizioni del D.Lgs 196/03 che prevede l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi individuati e dei modi per prevenire i danni.

In occasione delle riunioni, che saranno successivamente previste per la formazione, si provvederà anche alla valutazione ed alla revisione delle misure di sicurezza.

Le attività di formazione del personale incaricato e di revisione del presente documento vengono annotate in apposito registro verbale tenuto dal Responsabile del trattamento.

Il presente documento è stato illustrato ai docenti nella riunione del Collegio dei Docenti **del _____**, con particolare riferimento a quanto attiene alle documentazioni ed ai dati personali che vengono consegnati agli stessi e alle istruzioni date ai docenti incaricati del trattamento dei dati.

Data marzo 2007

Il titolare del trattamento
IL DIRIGENTE SCOLASTICO
 Dr. Anna Mennilli