

Anno scolastico 2009 2010

1. OGGETTO E AMBITO DI APPLICAZIONE

Il presente Documento Programmatico Sulla Sicurezza è redatto, ai sensi degli Artt. 33, 34, 35 e 36 D.L.svo n. 196/2003, per definire le politiche di sicurezza in materia di trattamento di dati personali ed i criteri organizzativi per la loro attuazione.

Il presente regolamento disciplina inoltre le modalità di accesso e di uso della rete informatica e telematica dello



ISTITUTO COMPRENSIVO TRINO
VIA VITTIME DI BOLOGNA N°4 - 13039 TRINO(VC)

TEL E FAX: 0161-801254

MAIL: SEGRETERIA@SCUOLETRINO.IT

ISTITUTOCOMPRENSIVO@SCUOLETRINO.IT

COD. FISC.: 94023440020 - COD. MEC.: VCIC80000E

e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire. La rete è connessa alla rete Internet tramite ADSL bilanciata.

L'istituto è diretto dalla dott.ssa Annamaria MARTINELLI e comprende:

SCUOLA SECONDARIA DI PRIMO GRADO "G.G. FERRARI" TRINO
SCUOLA PRIMARIA con sede a TRINO, PALAZZOLO e RONSECCO
SCUOLA DELL'INFANZIA con sede a TRINO, PALAZZOLO e TRICERRO

Tutti gli uffici amministrativi sono ubicati nella sede centrale in Via Vittime di Bologna n° 4 a Trino (VC)

1.1 PRINCIPI GENERALI – DIRITTI E RESPONSABILITÀ

Il Documento Programmatico sulla Sicurezza, in accordo con il Regolamento di attuazione delle norme sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali (da ora innanzi indicato come Regolamento), del quale si richiamano tutte le definizioni e disposizioni, definisce le politiche e gli standard di sicurezza in merito al trattamento dei dati personali.

Il Documento Programmatico sulla Sicurezza riguarda tutti i dati personali:

- Sensibili
- Giudiziari
- Comuni

Il Documento Programmatico sulla Sicurezza deve essere conosciuto ed applicato da tutti gli uffici dell' Istituzione scolastica e si applica al trattamento di tutti i dati personali per mezzo di:

- strumenti elettronici di elaborazione
- altri strumenti di elaborazione (es. cartacei, audio, visivi e audiovisivi, ecc.)

L'Istituzione scolastica promuove l'utilizzo della rete quale strumento utile per perseguire le proprie finalità.

Gli utenti manifestano liberamente il proprio pensiero nel rispetto dei diritti degli altri utenti e di terzi, nel rispetto dell'integrità dei sistemi e delle relative risorse fisiche, in osservanza delle leggi, norme e obblighi contrattuali.

Consapevoli delle potenzialità offerte dagli strumenti informatici e telematici, gli utenti si impegnano ad agire con responsabilità e a non commettere abusi aderendo a un principio di autodisciplina.

Il posto di lavoro costituito da personal computer viene consegnato completo di quanto necessario per svolgere le proprie funzioni, pertanto è vietato modificarne la configurazione.

Il software installato sui personal computer è quello richiesto dalle specifiche attività lavorative dell'operatore. E' pertanto proibito installare qualsiasi programma da parte dell'utente o di altri operatori, escluso l'amministratore del sistema. L'utente ha l'obbligo di accertarsi che gli applicativi utilizzati siano muniti di regolare licenza.

Ogni utente è responsabile dei dati memorizzati nel proprio personal computer. Per questo motivo è tenuto ad effettuare la copia di questi dati secondo le indicazioni emanate dal titolare del trattamento dei dati o suo delegato.

1.2 ABUSI E ATTIVITÀ VIETATE

E' vietato ogni tipo di abuso . In particolare è vietato:

usare la rete in modo difforme da quanto previsto dalle leggi penali, civili e amministrative e da quanto previsto dal presente regolamento;

utilizzare la rete per scopi incompatibili con l'attività istituzionale dell'Istituzione scolastica utilizzare una password di cui non si è autorizzati;

cedere a terzi codici personali (USER ID e PASSWORD) di accesso al sistema;

conseguire l'accesso non autorizzato a risorse di rete interne o esterne a quella Istituzione scolastica;

violare la riservatezza di altri utenti o di terzi;

agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;

agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);

fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);

installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (p.e. virus, cavalli di troia, worms, spamming della posta elettronica, programmi di file sharing - p2p);

installare o eseguire deliberatamente programmi software non autorizzati e non compatibili con le attività istituzionali;

cancellare, disinstallare, copiare, o asportare deliberatamente programmi software per scopi personali;

installare deliberatamente componenti hardware non compatibili con le attività istituzionali;

rimuovere, danneggiare deliberatamente o asportare componenti hardware.

utilizzare le risorse hardware e software e i servizi disponibili per scopi personali;

utilizzare le caselle di posta elettronica per scopi personali e/o non istituzionali;

utilizzare la posta elettronica con le credenziali di accesso di altri utenti;

utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi;

utilizzare l'accesso ad Internet per scopi personali;

accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;

connettersi ad altre reti senza autorizzazione;

monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;

usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;

inserire o cambiare la password del Bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;

abbandonare il posto di lavoro lasciandolo incustodito o accessibile.

1.3 ATTIVITÀ CONSENTITE

È consentito all'amministratore di sistema:

monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password;

rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;

rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

1.4 SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete l'Istituzione scolastica tutti i dipendenti, le ditte fornitrici di software per motivi di manutenzione e limitatamente alle applicazioni di loro competenza, collaboratori esterni impegnati nelle attività istituzionali per il periodo di collaborazione.

L'accesso alla rete è assicurato compatibilmente con le potenzialità delle attrezzature.

L'amministratore di sistema può regolamentare l'accesso alla rete di determinate categorie di utenti, quando questo è richiesto da ragioni tecniche.

Per consentire l'obiettivo di assicurare la sicurezza e il miglior funzionamento delle risorse disponibili l'amministratore di sistema può proporre al titolare del trattamento l'adozione di appositi regolamenti di carattere operativo che gli utenti si impegnano ad osservare.

L'accesso agli applicativi è consentito agli utenti che, per motivi di servizio, ne devono fare uso.

1.5 MODALITÀ DI ACCESSO ALLA RETE E AGLI APPLICATIVI

Qualsiasi accesso alla rete e agli applicativi viene associato ad una persona fisica cui collegare le attività svolte utilizzando il codice utente.

L'utente che ottiene l'accesso alla rete e agli applicativi si impegna ad osservare il presente regolamento e le altre norme disciplinanti le attività e i servizi che si svolgono via rete ed si impegna a non commettere abusi e a non violare i diritti degli altri utenti e dei terzi.

L'utente che ottiene l'accesso alla rete e agli applicativi si assume la totale responsabilità delle attività svolte tramite la rete.

L'utente è tenuto a verificare l'aggiornamento periodico del software antivirus.

Al primo collegamento alla rete e agli applicativi, l'utente deve modificare la password (parola chiave) comunicatagli dal custode delle password e rispettare le norme indicate nel paragrafo 10 del presente documento.

1.6 SANZIONI

In caso di abuso, a seconda della gravità del medesimo, e fatte salve ulteriori conseguenze di natura penale, civile e amministrativa, possono essere comminate le sanzioni disciplinari previste dalla normativa vigente in materia e dai regolamenti l'Istituzione scolastica".

2. MODALITÀ DI TRATTAMENTO DATI

In considerazione dei precedenti punti il Dirigente dell'Istituzione Scolastica, visto il decreto legislativo 30 giugno 2003, n. 196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 34 ss., nonché l'allegato B del suddetto D. Lgs., contenente il Disciplinary tecnico in materia di misure minime di sicurezza, è il titolare del trattamento dei dati.

Atteso che la suddetta Istituzione scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del D. Lgs. n. 196 del 2003, a-dotta il presente

2.1 DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

L'Istituzione scolastica, per l'espletamento della funzione didattica e formativa, raccoglie e tratta dati personali dei soggetti coinvolti nell'offerta formativa ovvero dei destinatari della stessa, anche con l'ausilio di soggetti esterni, si precisano a tal riguardo, i seguenti elementi:

1. Elenco dei trattamenti di dati personali;
2. Elenco dei dati personali di natura comune, sensibile o giudiziaria;
3. Distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

4. Ambito dei trattamenti;
5. Analisi dei rischi incombenti sui dati;
6. Misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
7. Criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
8. Programma degli interventi formativi degli incaricati del trattamento;
9. Criteri previsti per garantire il rispetto delle misure minime per i trattamenti di dati personali affidati all'esterno della struttura;
10. Trattamenti di dati personali sensibili o giudiziari con strumenti elettronici affidati all'esterno.

3. ELENCO DEI TRATTAMENTI DI DATI PERSONALI

Finalità

Al fine di perseguire le finalità istituzionali, l'Istituzione scolastica tratta dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori. I trattamenti sono effettuati, anche mediante strumenti elettronici, per le seguenti finalità:

adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi;

somministrazione dei servizi formativi;

gestione e formazione del personale, nelle sue varie componenti (docente e non docente, in ruolo presso altri apparati pubblici);

adempimenti assicurativi;

tenuta della contabilità;

gestione delle attività informative curate ai sensi della legge 7 giugno 2000, n. 150 contenente la "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni";

attività strumentali alle precedenti.

Fonte dei dati

I dati trattati sono conservati su supporti informatici e/o cartacei e sono noti all'istituzione scolastica, in ragione della produzione:

di atti e/o dichiarazioni provenienti da soggetti interessati a fruire direttamente, o a beneficio dei minori sottoposti alla potestà ex art. 316 c.c., dei servizi formativi;

documenti contabili connessi alla fornitura di prestazioni e/o di servizi e/o di lavori;

documentazione bancaria, finanziaria e/o assicurativa;

documenti inerenti il rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/o previdenziali.

4. ELENCO DEI DATI PERSONALI DI NATURA COMUNE O SENSIBILE

Sulla scorta delle precisazioni sopra elencate, l'istituzione scolastica, sulla base di una prima ricognizione, con salvezza della possibilità di procedere a successive integrazioni e/o correzioni entro il 31.12.2008, dichiara, con riferimento ai destinatari o familiari dei destinatari dell'offerta formativa ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo, coinvolti in rapporti negoziali con l'istituzione scolastica, o aspiranti ad assumere tale ruolo, di trattare i dati di seguito elencati:

Dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del D. Lgs. n. 196 del 2003, univocamente riconducibili ad un soggetto fisico, identificato o identificabile, quali nominativo, dati di nascita, residenza, domicilio, stato di famiglia, codice fiscale, stato relativo all'adempimento degli obblighi di leva.

Dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del D. Lgs. n. 196 del 2003, univocamente riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la sede, la Partita IVA, il Codice fiscale, la titolarità di diritti o la disponibilità di beni strumentali;

Dati sensibili, ai sensi dell'art. 4, comma 1, lett. d) del D. Lgs. n. 196 del 2003;

Dati giudiziari, ai sensi dell'art. 4, comma 1, lett. e) del D. Lgs. n. 196 del 2003;

Dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi individualizzati differenziati;

Dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;

Dati riferibili a procedimenti giudiziari, pendenti in qualsiasi grado, o pregressi, di natura civile, amministrativa, tributaria, presso autorità giurisdizionali italiane o estere, diversi da quelli rientranti nell'art. 4 comma 1, lett. e) del D. Lgs. n. 196 del 2003;

Dati atti a rilevare la presenza presso l'istituzione scolastica dei destinatari dell'offerta formativa ovvero dei famigliari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale offerta;

Dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;

Dati inerenti negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni;

Dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;

Dati contabili e fiscali;

Dati inerenti la titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;

Dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

5. DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI

L'ente titolare del trattamento dei dati, non **disponendo di personale interno con le caratteristiche richieste**, ha designato, mediante autonomo provvedimento, quale Responsabile ai sensi dell'art. 29 del D. Lgs. n. 196 del 2003,

preposto alle funzioni di **responsabile del trattamento dei dati informatici**, in considerazione della esperienza, capacità ed affidabilità espressa dalla medesima, tale da offrire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento.

Il sig. Verter Ferrari titolare della ditta P.Lion net

Il suddetto Responsabile del trattamento ha ricevuto adeguate istruzioni riguardo:

all'individuazione ed adozione delle misure di sicurezza da applicare nell'ambito dell'istituzione scolastica, al fine di salvaguardare la riservatezza, l'integrità, la completezza e la disponibilità dei dati trattati;

all'esigenza di provvedere, mediante atto scritto, all'individuazione delle unità legittimate al trattamento, per mezzo dei singoli preposti, ovvero di singoli incaricati, ai sensi dell'art. 30 del D. Lgs. n. 196 del 2003, deputati ad operare sotto la diretta autorità del responsabile, attenendosi alle istruzioni impartite, fermo restando l'obbligo gravante sul responsabile, di vigilare sul rispetto delle misure di sicurezza adottate;

all'esigenza di verificare che gli obblighi di informativa siano stati assolti correttamente, ovvero che sia stato conseguito il consenso degli interessati;

all'obbligo di collaborare con il titolare nell'adempiere alle richieste avanzate dal Garante per la protezione dei dati personali ovvero alle autorità investite dei poteri di controllo;

all'attribuzione della competenza ad elaborare e sottoscrivere notificazioni al Garante per la protezione dei dati personali;

all'obbligo di osservare e far osservare il divieto di comunicazione e diffusione dei dati personali comunque trattati da parte dell'istituzione scolastica;

all'obbligo, ovvero a proporre soluzioni organizzative che consentano un ampliamento dei livelli di sicurezza

Nomina inoltre il DSGA

Dott. Piero GHISIO

Responsabile del trattamento dei dati, che ai sensi dell'art. 30 del D. Lgs. n. 196 del 2003 e delle indicazioni rappresentate sub b), ha provveduto ad individuare gli incaricati, autorizzandoli al trattamento dei dati in possesso dell'istituzione scolastica, esclusivamente con riferimento all'espletamento delle funzioni istituzionali ad essi rispettivamente assegnate.

Tali incaricati, in particolare, sono stati formalmente edotti in merito alla circostanza che:

il trattamento e la conservazione dei dati deve avvenire esclusivamente in modo lecito e proporzionato alle funzioni istituzionali, nel rispetto della riservatezza;

la raccolta, registrazione ed elaborazione dei dati, mediante strumento informatico o cartaceo, deve essere limitata alle finalità istituzionali;

integra onere dell'incaricato la correzione od aggiornamento dei dati posseduti, l'esame della loro pertinenza rispetto alle funzioni

integra inosservanza delle istruzioni la comunicazione, effettuata in qualsiasi maniera dei dati in possesso, con eccezione del caso che il destinatario sia l'interessato alle stesse, ovvero altri soggetti legittimati ad ricevere dette comunicazioni.

L'ambito dei trattamenti autorizzati ai singoli incaricati è suscettibile di aggiornamento periodico.

A tutti gli incaricati destinati al 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. Con atto allegato al presente documento è stato designato l'incaricato della custodia delle copie di credenziali di autenticazione nonché della funzione di verifica del loro aggiornamento periodico ovvero della corretta utilizzazione.

Le suddette credenziali sono disattivate automaticamente dal gestore della rete periodicamente, ovvero in tutti i casi di mancata utilizzazione per almeno 6 (SEI) mesi.

Al fine di meglio precisare la suddetta ripartizione delle funzioni si rinvia alla tabella seguente:

Tabella 1 - Strutture preposte ai trattamenti e riparto delle responsabilità

STRUTTURA	TRATTAMENTI OPERATI DALLA STRUTTURA	COMPITI DELLA STRUTTURA
Ufficio Dirigente scolastico	Trattamenti strumentali allo svolgimento dei compiti istituzionali (gestione della corrispondenza ricevuta ed inviata dal Dirigente dell'istituzione scolastica;	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi

Ufficio Amministrativo	Trattamenti strumentali alla predisposizione e concreta erogazione dell'offerta formativa (raccolta delle domande di iscrizione; condizioni sanitarie ed economiche dei destinatari dell'offerta formativa, documentazione concernente opzioni per insegnamenti facoltativi, dati inerenti profili sanitari o relativi al nucleo familiare dei destinatari dell'offerta formativa, per il riconoscimento di attività di sostegno in ragione di situazioni di disagio, sociale, economico o familiare, registri relativi alle presenze presso l'istituzione scolastica)	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)
Ufficio DSGA	Trattamenti strumentali alle attività degli organi collegiali ed attività connesse ai rapporti con organi pubblici (composizione degli organi collegiali rappresentativi della comunità servita dall'offerta formativa, convocazione degli organi, raccolta delle delibere, raccolta degli atti concertati con altre istituzioni pubbliche)	Come sopra
Locale Server (coincide con il locale DSGA)	Trattamenti strumentali (interventi di carattere tecnico, aventi ad oggetto gli strumenti elettronici e i loro software)	Come sopra
Servizi strumentali, affidati all'esterno, concernenti l'assistenza e la manutenzione	Trattamenti strumentali (interventi di carattere tecnico aventi ad oggetto gli strumenti elettronici e i loro software, effettuati anche al di fuori dei locali di pertinenza dei singoli istituti scolastici)	Come sopra
Biblioteca	Gestione prestito d'uso dei libri	acquisizione e caricamento dei dati per i prestiti d'uso su cartaceo, consultazione delle schede di prestito libri

Archivio storico alunni	Archivio cartaceo degli alunni	Archiviazione dopo tre anni dalla fine del rapporto con l'istituzione scolastica. Consultazione, fotocopie, comunicazione a terzi
Archivio storico personale	Archivio cartaceo del personale docente e ATA	Come sopra
Archivio storico contabilità,	Archivio cartaceo della contabilità, bilancio di previsione, conto consuntivo, pratiche inps registri stipendi e TFR	Come sopra
Protocollo e archivio generale	Gestione delle circolari interne e della posta certificata ricevuta tramite fax, email, posta interna e posta ordinaria	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi, manutenzione tecnica dei programmi utilizzati nel trattamento, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.)

6. AMBITO DEI TRATTAMENTI.

Qui di seguito si precisano le modalità del trattamento dei dati nei vari uffici e sedi, mediante strumenti elettronici, secondo le modalità precisate nella tabella sottostante.

Tabella 2 - Elenco dei trattamenti: informazioni di base

Struttura deputata al trattamento	Natura dei dati trattati		Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
	Sensibili	Giudiziari			
Ufficio Dirigente scolastico			Ufficio Dirigente scolastico	Manutenzione interna o Ditta esterna, limitatamente alle esigenze di manutenzione e/o riparazione dei p.c interni e/o del server	Pc interno + server esterno
Ufficio amministrativo	X	X	Ufficio amministrativo	Come sopra	Pc interno + server esterno
Protocollo, Fax e Posta elettronica	X	X	Segreteria	Come sopra	Pc interno + server esterno
Archivio storico contabilità, protocollo	X	X	Stanza al pian terreno	Nessuna manutenzione	
Archivio storico personale	X	X	Stanza al pian terreno	Nessuna manutenzione	

Archivio storico alunni	X	X	Stanza al pian terreno	Nessuna manutenzione	
-------------------------	---	---	------------------------	----------------------	--

Il trattamento dei dati avviene attraverso modalità diverse: strumenti elettronici, in-terni (P.C.) ovvero collegati in rete fra loro, e/o mediante collegamenti alla rete intranet ed alla rete internet. Con riferimento alla gestione dei dati mediante rete ministeriale e RUPAR, l'Istituzione scolastica declina ogni responsabilità, operando come semplice utente, non essendo in grado di intervenire sulla gestione delle informazioni ivi contenute e gestite.

La tabella seguente riassume il quadro dei trattamenti secondo modalità e tipologia, precisando l'ubicazione dei supporti di memorizzazione.

Tabella 3 - Elenco dei trattamenti: descrizione degli strumenti utilizzati

IDENTIFICATIVO DEL TRATTAMENTO	EVENTUALE BANCHE DATI DI SUPPORTO	UBICAZIONE FISICA DEI SUPPORTI DI MEMORIZZAZIONE E DELLE COPIE DI SICUREZZA	TIPOLOGIA DI DISPOSITIVI DI ACCESSO	TIPOLOGIA DI INTERCON-NESSIONE
Ufficio Dirigente scolastico	Ruoli del personale e degli allievi in formato elettronico	Nei locali dell'Istituzione scolastica siti al Piano terra	PC	Rete locale e Internet
Ufficio DSGA	Ruoli del personale e dei progetti in formato elettronico	Come sopra	PC e schedario	Rete locale e Internet
Ufficio amministrativo	Ruoli del personale e degli allievi in formato elettronico Archivio degli allievi e genitori, Libretto assenze, faldoni con documentazione cartacea. Archivio contenuto negli elaboratori sottoposti a revisione o manutenzione da parte di tecnici, anche esterni, incaricati degli interventi (sia in caso di trasporto dell'elaboratore all'esterno dell'ente, presso i locali della ditta, sia in caso di intervento sul posto, cioè nei locali dell'istituzione scolastica).	Come sopra	PC e schedario	Rete locale e Internet
Archivio storico personale	Faldoni con materiale cartaceo	Nei locali dell'Istituzione scolastica siti al Piano seminterrato	Schedario	
Archivio storico alunni	Faldoni con materiale cartaceo	Come sopra	Schedario	
Archivio storico contabilità, protocollo	Faldoni con materiale cartaceo	Come sopra	Schedario	

7. ANALISI DEI RISCHI INCOMBENTI SUI DATI.

L'Istituzione scolastica ha proceduto ad una ricognizione dei rischi che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuito, in grado di recare pregiudizio ai dati personali trattati.

Le fonti di rischio sono state accorpate in:

Comportamenti degli operatori.

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

Eventi relativi agli strumenti.

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

Eventi relativi al contesto fisico-ambientale.

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

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

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

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

Tabella 4 - Analisi dei rischi

EVENTO		IMPATTO SULLA SICUREZZA DEI DATI		RIF. MISURE DI AZIONE
		DESCRIZIONE	GRA- VITÀ STI- MATA	
COMPORTAMENTI DEGLI OPERATORI	Furto di credenziali di autenticazione	Accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite
	Carenza di consapevolezza, disattenzione o incuria	Dispersione, perdita e accesso altrui non autorizzato	M	Formazione e flusso continuo di informazione
	Comportamenti sleali o fraudolenti	Dispersione, perdita e accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite

	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	M	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
EVENTI RELATIVI AGLI STRUMENTI	Azione di virus informatici o di codici malefici	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori;	EE	Adozione di idonei dispositivi di protezione
	Spamming o altre tecniche di sabotaggio	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	EE	Adozione di idonei dispositivi di protezione
	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico
	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	Adozione di idonei dispositivi di protezione
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	MA	Adozione di idonei dispositivi di protezione
EVENTI RELATIVI AL CONTESTO	Accessi non autorizzati a locali/reparti ad accesso ristretto	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori; accesso altrui non autorizzato	MB	Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	M	Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	A	Attività di controllo, assistenza e manutenzione periodica

	Errori umani nella gestione della sicurezza fisica	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	M	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
--	--	---	----------	---

8. MISURE ADOTTATE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI, NONCHÈ LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITÀ

Sulla scorta della ricognizione dei rischi sopra rappresentata, l'istituzione scolastica ha provveduto ad apprestare e/o introdurre strumenti di tutela, ovvero a prevedere incisive, misure di sicurezza. La tabella seguente sintetizza le misure di sicurezza in essere, corredate da indicazioni di dettaglio.

Tabella 5 - Le misure di sicurezza adottate o da adottare

MISURA	RISCHIO CONTRASTATO	STRUTTURA INTERESSATA	EVENTUALE BANCA DATI INTERESSATA	MISURA GIÀ IN ESSERE	PERIODICITÀ E RESPONSABILITÀ DEI CONTROLLI
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Ufficio Dirigente scolastico	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	semestrale; responsabile pro tempore del servizio
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Ufficio DSGA	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	semestrale; responsabile pro tempore del servizio
Preventiva, di contrasto, di contenimento degli effetti	Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Ufficio amministrativo	Relativo archivio	Antivirus, Firewall e credenziali di autenticazione	semestrale; responsabile pro tempore del servizio
Sala insegnanti	Perdita dati relativi ad anagrafiche, presenze e provvedimenti disciplinari insegnanti	Sala insegnanti	Registri di classe	Armadietti con chiavi personali (da ripristinare)	semestrale; responsabile pro tempore del servizio

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

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, si effettuano periodicamente dei salvataggi riguardanti i trattati. Sono state perciò acquisite licenze di uso per software antivirus. I documenti sono anche conservati in copia cartacea presso locali dell'istituzione scolastica non accessibili ai terzi e dotati di adeguati strumenti di protezione (armadi con serrature).

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

Tabella 6 - Salvataggio dei dati

SALVATAGGIO		CRITERI INDIVIDUATI PER IL SALVATAGGIO	UBICAZIONE DI CONSERVAZIONE DELLE COPIE	STRUTTURA OPERATIVA INCARICATA DEL SALVATAGGIO
STRUTTURA	DATI SENSIBILI O GIUDIZIARI CONTENUTI			
Ufficio Dirigente scolastico	- Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati - origine razziale o etnica - confessione religiosa	Salvataggio dati informatici giornalmente	Locale sito all'interno dell'ufficio del D.S.G.A.	Responsabile pro tempore del servizio
Ufficio DSGA	- Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati - origine razziale o etnica - confessione religiosa	Salvataggio dati informatici giornalmente	Locale sito all'interno dell'ufficio del D.S.G.A.	Responsabile pro tempore del servizio
Locale server	- Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati - origine razziale o etnica - confessione religiosa	Salvataggio dati informatici giornalmente	Locale sito all'interno dell'ufficio del D.S.G.A.	Responsabile pro tempore del servizio
Ufficio amministrativo	- Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati - origine razziale o etnica - confessione religiosa	Salvataggio dati informatici giornalmente	Locale a destra atrio ingresso.	Responsabile pro tempore del servizio e, per la parte di competenza dell'eventuale ditta esterna

Tabella 7 - Ripristino dei dati

RIPRISTINO (in seguito a distruzione o danneggiamento)		
DATA BASE/ARCHIVIO	SCHEDA OPERATIVA	PIANIFICAZIONE DELLE PROVE DI RIPRISTINO

Ufficio Dirigente scolastico	Viene effettuato un backup dei dati trattati e dei documenti che risiedono sul server tramite rete LAN, dal server ad un'altra macchina sita nell'ufficio D.S.G.A.	Semestrale
Ufficio DSGA	Come sopra	Semestrale
Ufficio amministrativo	Come sopra	Semestrale

10. MISURE DI CARATTERE ELETTRONICO/INFORMATICO

Le misure di carattere elettronico/informatico adottate sono:

utilizzo di server con configurazioni di ridondanza

Backup centralizzato effettuato settimanalmente e storico di un mese sul server per i programmi gestionali.

È attiva la definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000 e XP, di seguito specificate:

- a) la lunghezza della password deve essere almeno lunga 8 caratteri;
- b) deve possedere almeno un carattere numerico;
- c) non può essere ripetuta la precedente password;
- d) la password scade dopo un periodo di 3 mesi;

divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows 9x e Windows Me;

È attivo da parecchio tempo un sistema antivirus su tutte le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria;

definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;

definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate;

È attiva la separazione software della rete locale delle segreterie da quella dei laboratori didattici. A tale proposito si ricorda che il Sistema Informativo l'Istituzione scolastica dovrebbe essere costituito da due reti locali separate, quella didattica (dei laboratori e aule speciali) e quella amministrativa, rispettivamente composte da 56 e 7 posti di lavoro costituiti da personal computer Intel Pentium di varie potenze e capacità elaborative con sistemi operativi Windows 95/98, Windows2000 Professional e Windows XP.

Rete amministrativa (uffici)

Tutti i posti di lavoro sono connessi in rete locale. Tutti i personal computer (otto) sono riservati al personale dirigente e di segreteria. Il server di dominio viene utilizzato per il database dei dati relativi all'applicativo Sissi in rete.

La connettività internet avviene attraverso ADSL con indirizzo IP statico

La separazione/protezione tra la rete didattica e quella amministrativa è realizzata con Firewall

Rete didattica per i laboratori e aule speciali

La connettività internet avviene attraverso la connessione ADSL con indirizzo IP statico .

La separazione / protezione tra le reti (didattica e amministrativa) è realizzata in modo hardware.

11 REGOLE PER LA GESTIONE DELLE PASSWORD

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato user-id) e password personale.

User-id e password iniziali sono assegnati, dal custode delle password.

User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.

L'user-id è costituita dal cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.

La password è composta da almeno 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.

Ogni 3 mesi ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio u-ser-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

Le password verranno automaticamente disattivate dopo 6 mesi di non utilizzo.

Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.

In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio.

Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:

le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo o dopo operazioni di manutenzione;

per la definizione/gestione della password devono essere rispettate le seguenti regole:

la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;

deve contenere almeno un carattere alfabetico ed uno numerico;

non deve contenere più di due caratteri identici consecutivi;

non deve contenere lo user-id come parte della password;

al primo accesso la password ottenuta dal custode delle password deve essere cambiata; la nuova password non deve essere simile alla password precedente;

la password deve essere cambiata almeno ogni 3 mesi;

la password termina dopo 6 mesi di inattività;

la password è segreta e non deve essere comunicata ad altri;

la password va custodita con diligenza e riservatezza;

l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

11.1 REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICO/INFORMATICO

Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;

tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;

le copie di backup realizzate all'interno degli hard disk contenuti sul server e almeno una volta al mese vengono memorizzate su un CD e sono conservate in cassaforte contenuta presso l'ufficio del Dsga

divieto di utilizzare floppy disk come mezzo per il backup;

divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico almeno dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.

divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;

divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;

divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem e linee telefoniche senza specifica autorizzazione controfirmata dal Dirigente Scolastico.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Il fax si trova in locale ad accesso controllato (segreteria amministrativa) e l'utilizzo è consentito unicamente agli incaricati del trattamento.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata alle persone preposte solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

11.2 REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS

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

limitare lo scambio fra computer di supporti rimovibili (floppy, CD, Zip, hard disk rimovibili con interfaccia USB oppure 1394) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS;

controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;

evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento nella consapevolezza delle possibili conseguenze;

attivare la protezione massima per gli utenti del programma di posta Outlook al fine di proteggersi dal codice html di certi messaggi email (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);

non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");

non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);

non utilizzare le chat;

consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;

non attivare le condivisioni dell'Hard Disk in scrittura sulla partizione primaria denominata "C:".

seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);

avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito un malfunzionamento della rete o del PC (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);

conservare i dischi di ripristino del proprio PC in luogo sicuro e protetto (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);

conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;

conservare la copia originale del sistema operativo e la copia di backup consentita per legge;

conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore del sistema informatico o un suo delegato procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

formattare l'Hard Disk, definire le partizioni e reinstallare il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);

installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;

reinstallare i programmi applicativi a partire dai supporti originali;

effettuare il RESTORE dei soli dati a partire da una copia di backup recente. **NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP:** potrebbe essere infetto;

effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;

ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

11.3 INCIDENT RESPONSE E RIPRISTINO

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

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

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;

2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente. Una volta spento il sistema PC oggetto dell'incidente non deve più essere riacceso ;
4. documentare tutte le operazioni.

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

Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

1. eseguire una copia bit to bit degli hard disk del sistema compromesso;
2. se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
3. se l'incidente riguarda il sistema operativo il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

Tabella A - Procedure di spegnimento

Sistema operativo	Azione
MS DOS	<ol style="list-style-type: none"> 1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.
Windows 98/NT/2000/XP	<ol style="list-style-type: none"> 1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.

12. PROGRAMMA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO

L'istituzione scolastica intende aderire per il futuro alle iniziative formative organizzate dalla direzione regionale del Ministero dell'Istruzione dell'Università e della Ricerca Scientifica, tenendo anche conto dell'economicità di un'azione organizzata su base regionale, rispetto ad una gestione in proprio delle attività formative.

Nell'attesa delle iniziative di cui sopra l'Istituzione aderisce alle iniziative dell'associazione D-schola

13. VINCOLI CONTRATTUALMENTE ASSUNTI DAL FORNITORE ESTERNO AI FINI DELLA SICUREZZA DEI DATI

L'Istituzione scolastica non disponendo di professionalità interne **ha affidato all'esterno**, nei termini risultanti dalla sopraindicata tabella, i trattamenti di dati personali sensibili o giudiziari, effettuato con strumenti elettronici, previa assunzione da parte dell'affidatario – nell'ambito dello stesso contratto con cui viene realizzato l'affidamento o con atto aggiuntivo – degli impegni derivanti dalle seguenti dichiarazioni:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche ricevute per il trattamento dei dati personali e di integrarle nelle procedure già in essere;
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di avvertire (allertare) immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

14. ATTI E DOCUMENTI NON IN FORMATO ELETTRONICO, ARCHIVI CARTACEI

I trattamenti di dati personali con strumenti diversi da quelli elettronici sono effettuati dagli incaricati seguendo le istruzioni ad essi impartite, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. L'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati ha carattere annuale. Gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti. I medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solamente alle persone preventivamente autorizzate.

15. INTERVENTI DA ESEGUIRE ENTRO 31/12/2009

- 1) Consegnare i modelli relativi al trattamento dei dati personali, a tutti i dipendenti (ai sensi degli art. 33,34,35,36 del D.L.vo N. 196 del 30/06/2003) e conservare le ricevute restituite, firmate, in allegato al presente DPS.
- 2) Educare tutti i lavoratori che utilizzano videotermini all'uso corretto delle password (8 caratteri alfanumerici, non riconducibile a dati personali, importanza dello screen saver con password e tempo di attivazione <= dieci minuti) e relativa modifica consigliata ogni tre mesi ed obbligatoria ogni sei).
- 3) Confinare la macchina server all'interno di un armadio REC o comunque preservarlo dalla possibilità di contatti non controllati.
- 4) **Aggiungere nel modulo di iscrizione, nel riquadro relativo alla privacy, la postilla concernente la pubblicazione di foto/video degli allievi sul sito dell'Istituto.**
- 5) Ordinare l'archivio storico come da relative norme.

16. OBBLIGO DI AGGIORNAMENTO PERIODICO DEL DPS

Il presente documento programmatico sulla sicurezza è sottoposto a revisione annuale nella sua interezza, entro la scadenza del 31 marzo di ciascun anno, come previsto dalla regola 19 del Disciplinare tecnico di cui all'allegato B) al D.Lgs. 196/03, in relazione al disposto dell'art. 34, lettera g) del decreto stesso.

Il presente documento è aggiornato al 3/12/2009

IL TITOLARE DEL TRATTAMENTO

Dott. Annamaria MARTINELLI