

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del
D.L.vo N. 196 del 30/06/2003



MINISTERO DELLA PUBBLICA ISTRUZIONE UFFICIO SCOLASTICO REGIONALE PER LA TOSCANA

Scuola Secondaria Statale di I° Leonardo da Vinci
Via di Sotto, 1 - 50055 Lastra a Signa (FI)

Codice Fiscale: 80031110481
Codice Meccanografico: FIMM330008



DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Redatto ai sensi del Decreto Legislativo 30 giugno 2003, n. 196

Aggiornato al 31 marzo 2011

CODICE DELLA PRIVACY

(D.L.vo N. 196/2003)

DISPOSIZIONI MINIME SULLA SICUREZZA

E

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

Il presente documento si compone di n. 31 pagine

Prot. 1059/C2

Data di emissione: 14/03/2011

Il responsabile della sicurezza
Marcella Neri

(firma leggibile)

Scuola Secondaria Statale di I° Leonardo da Vinci
Via di Sotto, 1
50055 LASTRA A SIGNA (FI)

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Premessa

Scopo di questo documento è stabilire le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato da Scuola Secondaria Statale di I° Leonardo da Vinci, previsti dal D.L.vo 30/06/2003 Num. 196 "Codice in materia di protezione dei dati personali".

Il presente documento è stato redatto da DSGA, Neri Marcella. in qualità di Direttore Amministrativo, che provvede a firmarlo in calce.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

Normativa di riferimento

D.L.vo n. 196 del 30/06/2003;
Regolamento per l'utilizzo della rete.

Definizioni e responsabilità

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.

Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è la Scuola Secondaria Statale di primo grado Leonardo da Vinci e la titolarità è esercitata dal rappresentante legale Dirigente scolastico Prof. Cianti Luciano. Tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

Titolare, responsabili, incaricati

Titolare del trattamento: Dirigente scolastico Prof. CIANTI LUCIANO

Responsabile del trattamento dei dati: NERI MARCELLA

Responsabile della sicurezza informatica: figura non prevista

Amministratore della rete: NERI MARCELLA

Custode delle password: PICCHIO MARINA

Incaricati del trattamento dei dati: come da allegato 1

Incaricato dell'assistenza e della manutenzione degli strumenti elettronici: figura non prevista

Analisi dei rischi

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
 - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
 - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
 - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

Individuazione delle risorse da proteggere

Le risorse da proteggere sono:

- personale;
- dati/informazioni;

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

- documenti cartacei;
- hardware;
- software;

Elenco dei trattamenti dei dati personali

Finalità: Al fine di perseguire le finalità istituzionali, l'Istituzione Scolastica tratta dati personali (sia comuni che sensibili o giudiziari) di studenti e loro familiari, personale dipendente, fornitori di beni e prestatori di servizi, clienti. I trattamenti sono effettuati, anche mediante strumenti elettronici, per le seguenti finalità:

- adempimento agli obblighi di fonte legislativa, nazionale, territoriale o comunitaria, regolamentare o derivante da atti amministrativi;
- somministrazione dei servizi formativi;
- gestione e formazione del personale, nelle sue varie componenti comunque operanti nell'ambito scolastico;
- 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:

- 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 e amministrativi 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.

I dati trattati sono conservati su supporti informatici e/o cartacei e sono noti all'Istituzione Scolastica, in ragione della produzione e/o metodo di acquisizione

Elenco dei dati personali di natura comune e 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 31.3.2011*, 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:

- a. 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;
- b. 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;
- c. dati sensibili, ai sensi dell'art. 4, comma 1, lett. d) del d.lgs. n.196 del 2003;
- d. dati giudiziari, ai sensi dell'art.4, comma 1, lett. e) del d.lgs. 196/03;
- e. dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi individualizzati differenziati;

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

- f. dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;
- g. dati riferibili a procedimenti giudiziari, pendenti in qualsiasi grado, o pregressi, di natura penale, civile, amministrativa, tributaria, presso autorità giurisdizionali italiane o estere, compresi quelli rientranti nell'art. 4, comma 1, lett. e) del d.lgs. n.196 del 2003;
- h. dati atti a rilevare la presenza presso l'Istituzione Scolastica dei destinatari dell'offerta formativa ovvero dei familiari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale offerta;
- i. dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- j. 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;
- k. dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;
- l. dati contabili e fiscali;
- m. dati inerenti la titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;
- n. dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

Per ulteriori dettagli vedere gli Allegati 1 e 3.

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

L'Istituzione Scolastica nella persona del Dirigente Scolastico titolare del trattamento dei dati ha designato, mediante autonomo provvedimento (allegato al presente Documento) quale Responsabile ai sensi dell'art. 29 del d.lgs. n.196 del 2003 la Sig.ra NERI MARCELLA nata a BOLOGNA (BO) il 12/04/1973 in servizio in qualità di D.S.G.A FACENTE FUNZIONE in considerazione della capacità ed affidabilità possedute, tali da offrire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento (per la parte relativa al Personale ATA - UFFICI SEGRETERIA - DATI ALUNNI - PERSONALE - BILANCIO - MAGZZINO - FORNITORI), quale responsabile del trattamento dei dati.

I Responsabili del trattamento hanno 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.

Il Titolare del trattamento, ai sensi dell'art. 30 del d.lgs. n.196 del 2003 e delle indicazioni rappresentante sub b), ha provveduto ad individuare (mediante atti allegati al presente Documento) gli incaricati, autorizzandoli al trattamento dei dati in possesso dell'Istituzione Scolastica, esclusivamente con riferimento all'espletamento delle funzioni istituzionali ad essi

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

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;
- è onere dell'incaricato la correzione od aggiornamento dei dati posseduti, l'esame della loro pertinenza rispetto alle funzioni;
- è 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 a 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 mesi.

Può concorrere al trattamento anche una struttura esterna all'Istituzione Scolastica, incaricata mediante convenzione (da allegata alla presente nel caso), del supporto, manutenzione, riparazione degli strumenti elettronici. Il titolare della struttura è stato designato quale responsabile del trattamento, in ragione dell'esperienza maturata nel settore.

DATI TRATTATI DAI DOCENTI

Le banche dati cui hanno accesso più docenti sono:

- il registro di classe
- il registro dei verbali del consiglio di classe o di interclasse e collegio dei docenti.
- la documentazione relativa alla programmazione didattica
- i documenti di valutazione degli alunni
- la documentazione dello stato di handicap
- i certificati medici degli allievi
- la corrispondenza con le famiglie
- i documenti relativi agli alunni pervenuti dalle scuole di provenienza

Il trattamento dei dati da parte dei docenti è definito puntualmente da norme di legge o regolamentari.

DATI TRATTATI DAL PERSONALE COLLABORATORE SCOLASTICO

Il cartaceo contenenti dati personali a cui ha accesso il personale collaboratore scolastico, raggruppati in insiemi omogenei, sono:

- recapiti del personale
- recapito degli alunni
- e prestatori di servizi (distributori automatici, servizi assistenza)

DATI TRATTATI DAL PERSONALE AMMINISTRATIVO E TECNICO

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

- i fascicoli relativi al personale della scuola,
- i fascicoli degli alunni ed ex alunni
- l'anagrafe fornitori di beni e/o prestatori di servizi ed eventualmente clienti
- la documentazione finanziaria, contabile e amministrativa

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

- i contratti stipulati dall'Istituzione scolastica ovvero da questa detenuti
- il registro degli infortuni dipendenti ed alunni
- libri e documenti obbligatori D.Lgs 626/94 D.L.81/2008

DATI TRATTATI DAL DIRIGENTE SCOLASTICO

Le banche dati di pertinenza del Dirigente sono:

- il protocollo riservato
 - tutte le banche dati menzionate ai punti precedenti.

Individuazione delle minacce

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse.

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione	X	X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi		X	
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di acqua		X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		
Uso illegale di software	X	X	
Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	
Intercettazione (Eavesdropping)	X		
Infiltrazione nelle comunicazioni	X		
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Ripudio	X		
Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	

Per ulteriori dettagli delle minacce relative all'aspetto informatico vedere l'Allegato 2

Individuazione delle vulnerabilità

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nell'articolo 6.

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione inadeguata della rete
		Connessioni a linea pubblica non

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

		protette
--	--	----------

Documenti cartacei	Software	Personale
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione
	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

Individuazione delle contromisure

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico;
- contromisure di carattere procedurale;
- contromisure di carattere elettronico/informatico.

Contromisure di carattere fisico

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità del collaboratore scolastico di turno
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti;
- i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura del personale di segreteria e dei collaboratori scolastici
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area
- i locali attualmente sono provvisti di sistema di allarme e di estintore; la manutenzione del sistema di allarme è di competenza dell'ente locale.
- sono programmati interventi atti a dotare i locali ad accesso controllato di porte blindate,

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

armadi ignifughi, impianti elettrici dedicati, sistemi di condizionamento, apparecchiature di continuità elettrica (indicare quali interventi sono attivi, quali programmati).

Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal responsabile del trattamento o da un suo delegato;
- i visitatori occasionali delle aree ad accesso controllato sono accompagnati da un incaricato;
- per l'ingresso ai locali ad accesso controllato è necessaria preventiva autorizzazione da parte del Responsabile del trattamento e successiva registrazione su apposito registro;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri, contenenti dati comuni e particolari, durante l'orario di lavoro devono essere tenuti in e affidati al responsabile di turno. Al termine dell'orario di lavoro vengono depositati e successivamente raccolti da un incaricato del trattamento e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio dell'orario di lavoro.
- il responsabile del trattamento dei dati è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del responsabile del trattamento dei dati che è chiuso a chiave, una chiave di riserva è mantenuta con le dovute cautele;
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato nella cassaforte posta nella stanza del dirigente scolastico

Contromisure di carattere elettronico/informatico

Vedere l'Allegato 3.

Norme per il personale

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa, nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete (Allegato 4).

Incident response e ripristino

Vedere l'Allegato 3

Piano di formazione

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

Aggiornamento del piano

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Il presente piano è soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 Num. 196. Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

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

Elenco Allegati costituenti parte integrante di questo documento

- Allegato 1 - elenco trattamenti dei dati
- Allegato 2 - minacce hardware, minacce rete, minacce dati trattati, minacce supporti
- Allegato 3 - misure di carattere elettronico/informatico, politiche di sicurezza, incident response e ripristino
- Allegato 4 - regolamento per l'utilizzo della rete
- Lettere di incarico per il trattamento dei dati
- Lettera di incarico per il responsabile del trattamento
- Lettera di incarico per il custode delle password
- Lettera di incarico per l'amministratore di sistema

Il presente Documento Programmatico sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati.

Il redattore del documento
D.S.G.A. Marcella Neri

(firma leggibile)

Nota: Fonti di documentazione

Il modello di documento programmatico sulla sicurezza è stato predisposto consultando le seguenti fonti:

- **<http://www.garanteprivacy.it>**
- "Sicurezza informatica" ECDL IT Administrator - Modulo 5 Testo di riferimento per la certificazione EUCIP - McGraw Hill ISBN 88-3864333-4 Tabelle Minacce e vulnerabilità Cap. 1
- Il regolamento per l'utilizzo della rete è stato derivato dal documento CISEL 0203G286 - CISEL Centro Studi per gli Enti Locali - Maggioli

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

ALLEGATO 1 – Elenco trattamenti dei dati

Tabella 1 - Elenco dei trattamenti dei dati

Finalità perseguita o attività svolta	Categorie di interessati	Natura dei dati trattati	Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati
<p>Gestione delle iscrizioni e degli alunni.</p> <p>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, attività degli organi collegiali, composizione degli organi collegiali rappresentativi della comunità servita dall'offerta formativa, convocazione degli organi, raccolta delle delibere.</p>	Alunni e famiglie	Dati Personali sensibili / giudiziari / sanitari	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Moduli cartacei e fascicoli personali conservati in appositi schedari muniti di serratura e software ministeriale sul pc collegato in rete locale al server nel quale è conservato il database.
<p>Gestione del personale.</p> <p>Trattamenti strumentali allo svolgimento dei compiti istituzionali, in materia di selezione ed amministrazione del personale (registrazione delle presenze presso l'Istituzione Scolastica, assenze per malattia, esigenze familiari, espletamento funzioni politiche o sindacali; aspetti economici e previdenziali: paghe contributi, etc.; permessi per parcheggi interni; raccolta di curricula riguardo a soggetti</p>	Personale di ruolo e personale supplente	Dati Personali sensibili / giudiziari / sanitari	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Pc collegati in rete locale e materiale cartaceo conservato in appositi armadi e schedari muniti di serratura.

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

interessati all'espletamento di funzioni docenti)					
Gestione posta e protocollo. Trattamenti strumentali allo svolgimento dei compiti istituzionali (gestione della corrispondenza ricevuta ed inviata dal Dirigente dell'Istituzione Scolastica; tenuta del protocollo generale con conseguente registrazione della posta, anche elettronica o ricevuta via fax, e delle comunicazioni di ufficio in entrata e in uscita, attività connesse ai rapporti con organi pubblici e d enti esterni, raccolta degli atti concertati con altre istituzioni pubbliche	Tutti coloro che inoltrano comunicazioni alla scuola	Dati Personali semplici	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Protocollo informatico che viene periodicamente stampato e conservato agli atti della scuola. Schedari per la conservazione del cartaceo muniti di serratura. Programmi di posta elettronica. Gestione due indirizzi di posta elettronica, Istruzione, Pec.
Gestione contabile del personale	Supplenti e personale di ruolo	Dati Personali semplici/sensibili	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Pc collegato in rete al server sul quale è conservato il database relativo alle retribuzioni e alla gestione fiscale dei dipendenti.
Gestione del bilancio e dell'inventario. Trattamenti strumentali allo svolgimento dei compiti di gestione amministrativa (tenuta dei dati connessi all'espletamento di procedimenti amministrativi, attività contrattuale, gestione di beni, procedure di bilancio	Fornitori, revisori dei conti, sindacati	Dati Personali semplici	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Pc, software di gestione del Programma annuale e del Conto consuntivo.
Gestione della didattica	docenti e alunni	Dati Personali semplici/sensibili / sanitari	Sede didattica dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa		Registri di classe e registri degli insegnanti

Descrizione sintetica: menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es. gestione del personale, gestione collaboratori, gestioni clienti, gestioni fornitori, ecc.) e delle categorie di persone cui i dati si riferiscono (personale, collaboratori, clienti, fornitori, ecc.).

Natura dei dati trattati: indicare la classe di rischio dei dati trattati tenendo presente la seguente classificazione:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

- DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio;
- DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio
- DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

Struttura di riferimento: indicare la struttura (segreteria amministrativa, direzione, funzione svolta, ecc.) all'interno della quale viene effettuato il trattamento.

Altre strutture che concorrono al trattamento: nel caso in cui un trattamento, per essere completato, comporta l'attività di diverse strutture è opportuno indicare, oltre quella che cura primariamente l'attività, le altre principali strutture che concorrono al trattamento anche dall'esterno.

Descrizione degli strumenti utilizzati: va indicata la tipologia di strumenti elettronici impiegati (elaboratori o p.c. anche portatili, collegati o meno in una rete locale, geografica o Internet; sistemi informativi più complessi) e altre tipologie di contenitori (es. armadi, schedari...).

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Tabella 2 - Descrizione della struttura organizzativa

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Trattamento dei dati sensibili e non, riguardanti gli alunni, le famiglie, il personale, gli aspiranti inseriti nelle graduatorie, gli esperti esterni che vengono utilizzati per le attività della scuola, posta e protocollo, dati contabili e fiscali del personale.	Compiti di natura gestionale e organizzativa delle attività dell'istituzione. Acquisizione e caricamento dei dati degli alunni e del personale sui supporti informatici ministeriali, consultazione e modifica degli stessi, comunicazione a terzi (monitoraggi ministeriali, provinciali, comunali), manutenzione tecnica del software, gestione tecnica operativa della base dei dati (salvataggi settimanali o mensili, ripristini), conservazione del materiale cartaceo e informatico contenente i dati.
Sede didattica dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Erogazione del servizio di formazione agli alunni della scuola media.	Tenuta dei registri di classe. Tenuta dei registri personali per ogni insegnante. Gestione delle assenze degli alunni, raccolta dei certificati medici degli alunni a giustificazione delle assenze superiori a 5 giorni.

Struttura: riportare le indicazioni delle strutture menzionate nella Tabella 1.

Trattamenti effettuati dalla struttura: indicare i trattamenti di competenza di ciascuna struttura.

Compiti e responsabilità della struttura: descrivere sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza. Ad esempio: acquisizione e caricamento dei dati, consultazione, comunicazione a terzi, manutenzione tecnica dei programmi, gestione tecnica operativa della base dati (salvataggi, ripristini, ecc.).

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Tabella 3 - Elenco del personale incaricato del trattamento in ogni struttura e delle dotazioni informatiche.

Cognome e Nome	Struttura di riferimento	Strumenti utilizzati	Responsabilità aggiuntive
IEMMOLO GIORGIO	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	PC collegato in rete al server, registri informatici e cartacei relativi ai dati contabili dei dipendenti, conservati in appositi armadi.	Responsabile delle graduatorie personale scuola primaria e infanzia. Responsabile del backup del SISSI Responsabile delle graduatorie del personale scuola media e ATA. Custode delle password, conservate in cassaforte. Responsabile del fascicolo fiscale del personale dipendente. Responsabile dei rapporti con il CIP. Pratiche TFR. Responsabile del protocollo e del facile consumo
PICCHIO MARINA	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	PC collegato in rete al server, registri informatici e cartacei relativi ai dati degli alunni, conservati in appositi armadi muniti di serratura.	Responsabile del trattamento dei dati degli alunni, anche dati sensibili, riguardanti la salute, lo stato sociale, la religione. Custode delle chiavi delle casseforti con DSGA. Responsabile delle gite e viaggi d'istruzione. Collaborazione alla gestione del personale per pratiche relative alla pensione e ricostruzione di carriera
Docenti dell'istituto	Sede didattica dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Registri personali e registri di classe, PC non in rete	Trattamento dei dati degli alunni dei quali vengono a conoscenza per motivi didattici o nei colloqui con i genitori e con gli alunni stessi.
Collaboratori scolastici	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Telefono, fotocopiatrice, PC non in rete	Incaricati dei trattamenti dei dati degli alunni e del personale dei quali entrano a conoscenza per motivi di lavoro, nell'ambito delle proprie funzioni istituzionali.
NERI MARCELLA	Sede amministrativa direzionale dell'istituzione scolastica, Via di Sotto,1 Lastra a Signa	Pc collegato in rete al server sul quale è conservato il database. Armadi nei quali è conservato il materiale cartaceo relativo al programma annuale, al consuntivo e alla contabilità in generale, non forniti di serratura a lucchetto.	Responsabile del trattamento Custode delle chiavi delle casseforti
Dirigente scolastico Prof. CIANTI LUCIANO	Sede amministrativa direzionale dell'istituzione	Protocollo riservato. Pc collegato in rete Armadio nel	Titolare del trattamento

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

	scolastica, Via di Sotto,1 Lastra a Signa	quale è conservato il materiale, fornito di serratura a lucchetto.	
--	----------------------------------------------	--------------------------------------------------------------------------	--

Nome e cognome: riportare le indicazioni per ogni incaricato del trattamento.

Struttura di riferimento: riportare l'indicazione della struttura di appartenenza di ogni incaricato.

Strumenti utilizzati: per ogni incaricato riportare le informazioni relative allo strumento utilizzato (p.e. numero di inventario del PC).

Responsabilità aggiuntive: indicare le eventuali responsabilità aggiuntive rispetto all' incarico per il trattamento dei dati, ad esempio "responsabile del trattamento", "responsabile delle copie di backup", "custode delle chiavi di un contenitore o armadio", "custode delle password", ecc.

Nota: parte delle indicazioni sono tratte dalla "Guida operativa per redigere il documento programmatico sulla sicurezza (DPS)" pubblicate dal garante

ALLEGATO 2 – Minacce

Minacce a cui sono sottoposte le risorse hardware

Le principali minacce alle risorse hardware sono:

- malfunzionamenti dovuti a guasti;
- malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;
- malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

Minacce a cui sono sottoposte le risorse connesse in rete

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

all'utilizzo della LAN/Intranet (internet);

ai punti di contatto con il mondo esterno attraverso Internet (esterne);

- allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interne/esterne).

In dettaglio si evidenziano le seguenti tecniche:

IP spoofing

L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.

Packet sniffing

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

Port scanning

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

Highjacking

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

Social engineering

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

Buffer overflow

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

Spamming

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

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

Password cracking

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

Trojan

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

Worm

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

Logic bomb

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

Malware e MMC (Malicious Mobile Code)

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

DOS (Denial of Service)

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

DDOS (Distributed Denial of Service)

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

L'utilizzo di programmi di sniffing e port scanning é riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete locale LAN, tali programmi non sono in nessun caso utilizzati su reti esterne a quella della rete locale LAN.

La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dalla Autorità Giudiziaria.

Minacce a cui sono sottoposti i dati trattati

Le principali minacce ai dati trattati sono:

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

Minacce a cui sono sottoposti i supporti di memorizzazione

Le principali minacce ai supporti di memorizzazione sono:

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

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

ALLEGATO 3 – Misure, incident response, ripristino

Tabella 1 - Connettività internet

Connettività	Apparecchiature di comunicazione	Provider
ADSL	Router	Telecom - Alice

Connettività: indicare il tipo di connettività internet (XDSL, ISDN, PSTN).

Apparecchiature di comunicazione: indicare il tipo di apparecchiature utilizzate per la connettività (modem, router).

Provider: indicare il fornitore di connettività.

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Tabella 2 - Descrizione Personal Computer

Identificativo del PC	Tipo PC	Sistema operativo	Software utilizzato	Rete
PC DSGA	Assemblati	Windows XP	Office, Sissi, Opensissi, Fisco ol-line, Entratel, Pre1996, Adobe pdf, INPS Emens, Easyprint	lan
PC Marina	Assemblato	Windows XP	Office, Sissi, Opensissi, INPS Emens, Entratel, Pre1996, Adobe pdf, easyprint	lan
PC Giorgio	Assemblato	Windows XP	Office, Sissi, Opensissi, INPS Emens, Entratel, Pre1996, Adobe pdf, easyprint.	lan
PC Dirigente	Assemblato	Windows XP	Office, Sissi, Opensissi, E Adobe pdf	lan
PC Protocollo	Assemblato	Windows XP	Office, Sissi, Opensissi, Adobe pdf.	lan
PC Remo	Assemblato	Windows XP	Office, Sissi, Adobe pdf, Easyprint.	lan
PC Sala docenti	Assemblato	Windows XP	Office.	lan
PC C.S.	Assemblato	Windows XP	Office.	lan

Identificativo del PC: indicare l'elenco di tutti i PC utilizzati sia connessi che non connessi alla rete (per esempio con il numero di inventario).

Tipo PC: indicare il tipo del PC.

Sistema operativo: indicare quale Sistema operativo è utilizzato sul PC.

Software utilizzato: indicare il software applicativo utilizzato per il lavoro (es. OFFICE, STAROFFICE, ecc...).

Rete: indicare se il PC è connesso alla rete.

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Misure di carattere elettronico/informatico

Le misure di carattere elettronico/informatico adottate sono:

- utilizzo di server con configurazioni di ridondanza (indicare se la misura è attiva o entro quando sarà adottata). La misura è correttamente attuata infatti sul server sono presenti due hd in mirror.
- presenza di gruppi di continuità elettrica per il server (indicare se la misura è attiva o entro quando sarà adottata); è attiva
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità settimanale e storico di un mese (indicare se la misura è attiva o entro quando sarà adottata). Alla data di questo documento i responsabili delle copie sono indicati nell'Allegato 1 relativo al censimento dei trattamenti dei dati; il back up è effettuato mensilmente sul sistema Sissi. È attiva la procedura di back up giornaliero sui documenti comuni sul server, oltre che del database del Sissi.
- installazione di un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet (indicare se la misura è attiva o entro quando sarà adottata); È presente un firewall all'accesso alla rete.
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000 , XP e VISTA, SEVEN di seguito specificate (indicare se la misura è attiva o entro quando sarà adottata); tutte le macchine sono dotate di password di accesso che sono modificate ogni 6 mesi e che sono depositate attraverso il custode delle password nella cassaforte della scuola.
- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows;
- è installato di 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
- Risulta installato il software antivirus " McAfee" su tutte le macchine, con l'attivazione dell'aggiornamento automatico giornaliero.
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate: credenziali di accesso, firewall, antivirus.
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate: non utilizzare supporti di derivazione personale sulle macchine dell'ufficio.

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

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.

La User-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.

La password è composta da 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 sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-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 tre 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. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.

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

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

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

- la password deve essere costituita da una sequenza di minimo sei 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 sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
- la password termina dopo sei 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

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

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;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su cassetta Yomega (indicare il dispositivo, CD, cassetta, ecc...) sono conservate nel cassetto nell'ufficio della DSGA (specificare il tipo di contenitore es. armadio chiuso a chiave , e indicare la sua ubicazione)
- 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 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.
- Il fax si trova in locale ad accesso controllato e l'utilizzo è consentito unicamente agli incaricati del trattamento (Aa.Aa. e Cc.Ss.)

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.

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata 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.

Regole di comportamento per minimizzare i rischi da virus

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

- *divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;*
- *limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) 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;*
- *disattivare gli ActiveX e il download dei file per gli utenti del browser Internet Explorer;*
- *disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);*
- *attivare la protezione massima per gli utenti del programma di posta Outlook Express al*

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

fine di proteggersi dal codice html di certi messaggi e-mail (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'HD in scrittura.*
- *seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);*
- *avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);*
- *conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);*
- *conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;*
- *conservare la copia originale del sistema operativo e la copia di backup consentita per legge;*
- *conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).*

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

- *formattare l'Hard Disk,definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);*
- *installare il software antivirus, verificate 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.*

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

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(vedi tabella 3). Una volta spento il sistema oggetto dell'incidente non deve più essere riaccessato;
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:

- eseguire una copia bit to bit degli hard disk del sistema compromesso;
- 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;
- se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC (vedere Allegato 2) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

Tabella 3 - 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.
UNIX/Linux	<ol style="list-style-type: none">1. Fotografare lo schermo e documentare i programmi che sono attivi.2. Se la password di root è disponibile eseguire il comando su e poi i comandi sync e halt.3. Se la password di root non è disponibile staccare la spina dalla presa di corrente.
Mac	<ol style="list-style-type: none">1. Fotografare lo schermo e documentare i programmi che sono attivi.2. Cliccare Special.3. Cliccare Shutdown.4. Una finestra indicherà che è possibile spegnere il sistema.5. Staccare la spina dalla presa di corrente.
Windows 98/NT/2000/XP/VISTA	<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.

Nota: (fonte U.S. Departement of Energy)

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

ALLEGATO 4 - Regolamento per l'utilizzo della rete

Oggetto e ambito di applicazione

Il presente regolamento disciplina le modalità di accesso e di uso della rete informatica e telematica e dei servizi che, tramite la stessa rete, è possibile ricevere o offrire.

Principi generali - diritti e responsabilità

La scuola secondaria statale di primo grado Leonardo da Vinci 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.

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;
- utilizzare una password a 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;
- 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 distruggano 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;

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

- 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, come specificato nell'allegato 3.

Attività consentite

E' 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 come da procedura descritta nell'allegato 3;
- 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.

Soggetti che possono avere accesso alla rete

Hanno diritto ad accedere alla rete 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

Documento programmatico sulla sicurezza

ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003

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.

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 nell'allegato 3.

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 interni.