

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)

ISTITUTO...

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 dall' **ISTITUTO....**, 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 ... *(indicare chi)*. in qualità di **responsabile della sicurezza**, 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.

Articolo 1

NORMATIVA DI RIFERIMENTO

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

Articolo 2

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

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)

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 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 l'Ente (ISTITUTO SCOLASTICO) e la titolarità è esercitata dal rappresentante legale (DIRIGENTE SCOLASTICO), 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.

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)

Articolo 3

TITOLARE, RESPONSABILI, INCARICATI

Titolare del trattamento: ... *(indicare chi)*

Responsabile del trattamento dei dati: ... *(indicare chi)*

Responsabile della sicurezza informatica: ... *(indicare chi)*

Amministratore della rete: ... *(indicare chi)*

Custode delle password: ... *(indicare chi)*

Incaricati del trattamento dei dati: come da allegato 1

Incaricato dell'assistenza e della manutenzione degli strumenti elettronici: ... (indicare chi)

Articolo 4

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.

Articolo 5

INDIVIDUAZIONE DELLE RISORSE DA PROTEGGERE

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;

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)

- software;
- apparecchiature di comunicazione;
- **manufatti vari;**
- **servizi;**
- **apparecchiature per l'ambiente;**
- immagine della scuola.

Per ulteriori dettagli vedere gli Allegati 1 e 3.

Articolo 6 **INDIVIDUAZIONE DELLE MINACCE**

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse indicate all'articolo 5.

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	
Interruzione di aria condizionata	X	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	

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)

Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
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

Articolo 7 **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	Mancanza di autenticazione

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)

	temperatura	
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 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	

Articolo 8 **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

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)

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 dell' **ISTITUTO.....**;
- 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 di;
- **l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'ISTITUTO.....;**
- i locali sono provvisti di sistema di allarme e di estintore *(indicare se le misure sono attive o entro quando lo saranno)*;
- **sono programmati interventi atti a dotare i locali ad accesso controllato di porte blindate, 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 della 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 allarmi e 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 di classe, contenenti dati comuni e particolari, durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni vengono depositati dall'insegnante dell'ultima ora di lezione *(indicare dove)* e successivamente raccolti da un incaricato del trattamento e conservati in luogo sicuro per essere riconsegnati da un incaricato del trattamento all'inizio delle lezioni.

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 docente 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 docente che è chiuso a chiave, una chiave di riserva è mantenuta con le dovute cautele dalla scuola (*indicare dove*);
- il protocollo riservato, accessibile solo al Titolare e al Responsabile del trattamento è conservato (*indicare dove*);
- inoltre per il trattamento dei soli dati cartacei sono adottate le seguenti disposizioni:
 - si accede ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
 - si utilizzano archivi con accesso selezionato;
 - atti e documenti devono essere restituiti al termine delle operazioni;
 - è fatto divieto di fotocopiare/scannerizzare documenti senza l'autorizzazione del responsabile del trattamento;
 - è fatto divieto di esportare documenti o copie dei medesimi all'esterno dell'**Istituto** senza l'autorizzazione del responsabile del trattamento, tale divieto si estende anche all'esportazione telematica;
 - il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti deve essere ridotto in minuti frammenti.

Contromisure di carattere elettronico/informatico

Vedere l'Allegato 3.

Articolo 9 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 e indicate nell'articolo 5 , nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete (Allegato 4).

Articolo 10 INCIDENT RESPONSE E RIPRISTINO

Vedere l'Allegato 3

Articolo 11 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

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;

- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

(Indicare se la formazione è stata fatta e da chi o quando sarà effettuata)

Il piano prevede inoltre la pubblicazione di normativa ed ordini di servizio in **apposita** bacheca situata **in ufficio (specificare dove)**.

Articolo 12

AGGIORNAMENTO DEL PIANO

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 scuola 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 scuola tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

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)

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
- Allegato 5 – uso del proxy (eliminare se non si utilizza)
- Allegato 6 – attività di videosorveglianza (eliminare se non si utilizza)
- 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.

LUOGO E DATA

Il redattore del documento
(NOME COGNOME)

(firma)

Nota: Fonti di documentazione

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

- <http://www.garanteprivacy.it>
- <http://www.osservatoriotecnologico.net>
- "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 proposto alla Giornata di studio CISEL 0203G286 – CISEL Centro Studi per gli Enti Locali – Maggioli