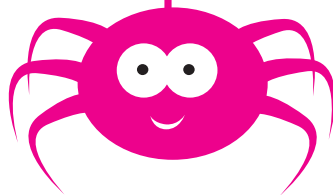


Doriano Azzena - Giovanni Marcianò - Barbara Petrella
Michele Tortorici



UN RAGNO PER AMICO 2

USO CONSAPEVOLE
DELLE NUOVE TECNOLOGIE
E SICUREZZA DEI DATI

**MIUR - Ufficio Scolastico Regionale per il Piemonte
Ottobre 2004**

Ringraziamenti:

Gruppo SisCAS

Michele Maffucci per il sito www.siscas.net/dps

Fonti di documentazione:

La bozza di documento programmatico sulla sicurezza è stata predisposta 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

Quaderni pubblicati dall'Ufficio Scolastico Regionale per il Piemonte del MIUR

Direttore: Luigi Catalano

Direttore Editoriale: Michele Tortorici

Responsabile Editing: Servizio per la Comunicazione dell'Ufficio scolastico regionale per il Piemonte

Il presente quaderno potrà essere riprodotto per l'utilizzo da parte delle scuole in attività di formazione del personale direttivo, docente e ATA. Non potrà invece essere riprodotto né parzialmente né totalmente per realizzare altre pubblicazioni o per usi diversi da quelli sopraindicati, salvo autorizzazione scritta dell'Ufficio scolastico regionale per il Piemonte.

Edizione fuori commercio

Tutti i volumi della collana dei “Quaderni” sono scaricabili in formato PDF dall'indirizzo www.piemonte.istruzione.it/quaderni_USR.shtml e/o possono essere richiesti a USR Piemonte - Via Pietro Micca, 20 - 10122 Torino



INDICE



Policy d'uso sicuro delle TIC e protezione dei dati	pag. 5
--	--------

NORMATIVA

Linee di indirizzo dell'U.S.R. Piemonte	pag. 7
Normativa nazionale	pag. 11

GUIDA ALLA COMPILAZIONE DEL DPS

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)	pag. 13
Allegato 1 - elenco trattamenti dei dati	pag. 27
Allegato 2 - minacce	pag. 30
Allegato 3 - misure, incident response, ripristino	pag. 34
Allegato 4 - regolamento per l'utilizzo della rete	pag. 42
Allegato 5 - utilizzo del proxy	pag. 46
Allegato 6 - videosorveglianza	pag. 48
Incarico per il trattamento dei dati	pag. 49
Incarico di responsabile del trattamento dati	pag. 51
Incarico custode delle password	pag. 52
Incarico di amministratore di sistema	pag. 53
Incarico di responsabile della sicurezza informatica	pag. 54
Incarico per il trattamento di dati personali ai docenti	pag. 55
Informativa (ai sensi dell'art. 13 D. L.vo 196/2003)	pag. 59
Consenso al trattamento dei dati (art. 23 D. L.vo 196/2003)	pag. 61
Richiesta di comunicazione e diffusione di dati sugli esiti scolastici nell'interesse dell'alunno (ex art. 96 D.L.vo 196/03)	pag. 62

GLOSSARIO

Termini ricorrenti	pag. 63
---------------------------	---------



L'Ufficio scolastico regionale per il Piemonte, nell'ambito delle strategie sviluppate dal MIUR, ha da tempo individuato nel sistematico ricorso alle nuove tecnologie uno degli strumenti determinanti per garantire a livello regionale la funzionalità del sistema scuola. Ha perciò offerto servizi e strumenti alle scuole del Piemonte per consentire loro di svolgere al meglio i compiti impegnativi che le attendono aprendosi alle esigenze degli operatori del mondo della scuola anche e soprattutto attraverso l'utilizzo di internet.

L'autonomia scolastica ha inciso in questi anni in profondità nel modo delle scuole di partecipare alla vita dell'amministrazione e anche l'Ufficio scolastico regionale ha modificato la sua visione scegliendo di essere uno dei soggetti in campo, di porsi a fianco delle scuole e di concorrere allo scambio comunicativo necessario a far vivere la loro autonomia: tutto ciò insieme agli altri attori istituzionali (in primo luogo) e sociali che agiscono sul terreno culturale e della formazione.

In questo scenario l'Ufficio scolastico regionale riafferma l'importanza dello sviluppo di una cultura di utilizzo consapevole delle nuove tecnologie.

Questo quaderno si offre come strumento di uso facile e immediato per comprendere la materia della sicurezza nel trattamento dei dati e per supportare le istituzioni scolastiche nell'assolvimento di alcuni obblighi derivanti dalle norme del Codice in materia di protezione dei dati personali e nella redazione del Documento programmatico sulla Sicurezza. Di proposito si è usata, come nel Quaderno 7 (dedicato alle Indicazioni alle scuole per usare bene e in sicurezza internet e LAN), una forma grafica accattivante volta a favorire il contatto con questa materia un po' ostica e a renderla di più facile accesso. Così come nel precedente, anche in questo Quaderno la mascotte Ragno è chiamata a mostrare che l'utilizzo consapevole delle nuove tecnologie permette di addentrarsi nella "rete" senza paura di restarne vittime.

Possiamo anche aggiungere che il Ragno non è più solo. Mentre questa mascotte accompagna le scuole a muoversi sicure in rete, un altro personaggio - il Capitano - aiuta a navigare, a comunicare e a fare ricerca in modo sicuro in Internet.

È stata proprio la pubblicazione del Quaderno 7 a ispirare gli autori di un nuovo browser italiano sicuro, "Il Veliero". Il protocollo d'intesa sottoscritto nel luglio 2004 dall'USR Piemonte e dalla casa produttrice ha poi permesso di coinvolgere in prima persona la scuola piemontese nello sviluppo del browser "Il Veliero scuola", oggi in via di consegna alle scuole primarie della regione, che per l'anno scolastico corrente, potranno impiegarlo gratuitamente nel laboratorio d'Istituto. L'uso di Internet, senza troppi tecnicismi, ma con la garanzia della massima sicurezza possibile, viene messo così al servizio della programmazione didattica di ogni insegnante delle scuole dell'infanzia ed elementari e, in parte, anche della secondaria di primo grado.

Lungo il cammino che l'Ufficio scolastico regionale compie da tempo per affiancare le scuole nel creare una serie articolata e integrata di strumenti destinati a facilitare alle scuole l'uso delle TIC, questo quaderno costituisce un passo ulteriore e si presenta come una sorta di "aggiunta" e "integrazione" del primo Ragno per amico. D'altro canto, qualsiasi misura riguardante la sicurezza nel trattamento dei dati sarebbe inefficace se non si inserisse all'interno di una



cultura generale della prevenzione e va quindi considerata soltanto come una parte di quella più generale policy di uso sicuro delle tecnologie e della rete che costituisce la tematica del quaderno precedente.

Il Ragno guida attraverso le tre sezioni del quaderno:

- Normativa (regionale e nazionale)
che contiene la Circolare Regionale nr. 253 del 21 ottobre 2004 e un elenco delle principali norme relative alla materia del trattamento dei dati personali
- Guida alla compilazione del DPS
che contiene un fac-simile di Documento programmatico sulla sicurezza strutturato in un esempio base, 6 allegati e modelli di lettere di incarico.
- Glossario
che contiene la spiegazione del significato dei termini di uso ricorrente

L'Ufficio scolastico regionale per il Piemonte ha creato il sito www.siscas.net/dps per dare alle istituzioni scolastiche la possibilità di utilizzare i modelli nella forma più agile per la compilazione. Le scuole possono scaricare i vari documenti in formato RTF e modificarli direttamente. Nel sito è possibile anche trovare tutte le norme che in questo quaderno vengono solo elencate.

È inoltre ancora aperto il forum "UsoSicuro" (<http://www.siscas.net/forum/usosicuro>), uno spazio di discussione sui diversi fronti della sicurezza informatica nel quale, tra l'altro, si possono trovare i lavori delle insegnanti che hanno collaborato alla ricerca azione online sul "Veliero" e la registrazione delle loro prime esperienze in classe.



Linee di indirizzo dell'Ufficio scolastico regionale per il Piemonte

Circolare Regionale N° 253 del 21 ottobre 2004

- Ai Dirigenti Scolastici
delle scuole statali e paritarie
di ogni ordine e grado
della regione Piemonte
LORO SEDI
- e p.c. Ai Dirigenti dei CSA
dell'USR per il Piemonte
LORO SEDI
- e p.c. Ai Dirigenti Tecnici e Amministrativi
dell'USR Piemonte
LORO SEDI

Oggetto: obbligo di protezione dei dati personali nel nuovo Codice della Privacy (D.L.vo 196/2003)

Le scuole e le istituzioni educative possiedono banche dati in cui sono conservate e indicizzate notizie e informazioni personali riguardanti gli alunni e i dipendenti. La riservatezza di questi dati deve essere garantita almeno al "livello minimo di protezione e sicurezza". Il trattamento dei dati personali deve svolgersi, infatti, nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato. Le norme del Decreto legislativo 196 del 2003, denominato "Codice in materia di protezione dei dati personali", riguardano quindi un aspetto fondamentale della vita civile e fanno particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. Esse ci ricordano che chiunque ha diritto a veder garantita la sicurezza dei dati personali che lo riguardano.

Il "Codice in materia di protezione dei dati personali" ha introdotto nuove garanzie per i cittadini, ha razionalizzato le norme esistenti e ha semplificato gli adempimenti necessari. Rappresenta perciò il primo organico tentativo di riorganizzare le innumerevoli disposizioni relative alla riservatezza personale - o privacy - e riordina in un unico contesto le norme a suo tempo dettate dalla legge 675/1996 e dagli altri regolamenti e codici che si sono succeduti in questi anni.

Rispetto a questa realtà il sistema educativo deve agire, come sempre, con la capacità di trasformare in occasione educativa anche questi adempimenti normativi apparentemente aridi, ma legati - è necessario non dimenticarlo - alla fruizione da parte del cittadino di una specifica dimensione dei suoi diritti. L'autonomia consente infatti oggi a tutte le scuole di svolgere a pieno titolo, nel campo dell'educazione e della cultura, un nuovo ruolo di soggetto sociale.



In tutti i campi, e in particolare in quello che riguarda l'uso delle tecnologie e il trattamento dei dati, i soggetti che agiscono in maniera forte sulla crescita dei nostri giovani sono tanti e tanti di essi sono fuori della scuola stessa; ma, nel nuovo ruolo che hanno assunto, sono proprio le scuole che hanno il compito di far rifluire i molteplici stimoli in un organico processo di crescita e di dare senso a questi stimoli.

Con l'autonomia le scuole sono chiamate a esercitare la loro funzione culturale non separandosi da ciò che avviene intorno a loro, ma costituendosi come "filtro" e, proprio per questo, immergendosi esse stesse nella realtà, con la finalità di definire gli obiettivi di apprendimento non più in rapporto alle conoscenze, ma - lo dice esplicitamente l'articolo 8 del Regolamento dell'Autonomia - in rapporto alle competenze, cioè al modo in cui le conoscenze stesse vengono non solo possedute, ma padroneggiate e, soprattutto, utilizzate in un contesto dato.

Nel perseguire questi fini le istituzioni scolastiche hanno rafforzato il loro status di Amministrazioni pubbliche. Nel prendere coscienza di tutta la problematica relativa all'introduzione delle nuove norme sulla protezione dei dati personali, rispondono quindi a un impegno di carattere didattico e culturale e assolvono al tempo stesso a un dovere di ordine amministrativo. La duplice natura di questa azione è insita nel loro stesso codice genetico.

In questa prospettiva, le istituzioni scolastiche costituiscono la sede primaria, istituzionale e strategica nella quale avviare un processo allargato di partecipazione, indirizzo e sensibilizzazione complessiva degli operatori scolastici e dei cittadini (gli alunni e le loro famiglie) in relazione alla sicurezza nel trattamento dei dati, non limitandosi a interventi e adempimenti di carattere meramente formale ovvero a iniziative sporadiche e occasionali.

D'altra parte l'attuale normativa induce a considerare la sicurezza informatica, e la sua gestione nei numerosi campi che essa investe, non più come un'utile possibilità, ma come un obbligo e costituisce un'opportunità per la promozione, a livello scolastico, di una vera e propria cultura della sicurezza e della prevenzione.

La risoluzione del problema della protezione dei dati personali passa attraverso le seguenti fasi:

1. analisi della normativa;
2. analisi del sistema organizzativo attualmente in opera in materia di gestione dei dati personali e sensibili in tutte le modalità e su tutti i supporti;
3. analisi del sistema informatico attualmente in opera per la gestione dei dati in formato digitale;
4. predisposizione delle misure minime di sicurezza dei dati;
5. esecuzione di tutti gli adempimenti formali;
6. gestione delle fasi successive di evoluzione della norma.

Il D. Lgs. 196/2003 individua i seguenti obblighi (Artt. 11, 13, 20, 22, 33, 34 e 35 e allegato B), oltre a quelli formali di nomina del responsabile o dei responsabili e degli incaricati:

1. obbligo di informativa nei confronti dell'interessato;



2. obbligo di conservare e controllare i dati personali oggetto di trattamento per evitare il rischio che siano distrutti, dispersi anche accidentalmente, conoscibili anche fuori dei casi consentiti o trattati in modo illecito.
3. obbligo di adottare misure minime di sicurezza, che sono diverse a seconda che il trattamento sia effettuato o meno con strumenti elettronici, oppure se riguardano i dati sensibili.

Se i dati vengono trattati con strumenti elettronici occorre adottare le seguenti **misure minime di sicurezza**:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- individuazione e aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- **tenuta di un aggiornato documento programmatico sulla sicurezza**;
- previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. Dopo il primo intervento, la formazione è programmata al momento dell'ingresso in servizio di nuovo personale, nonché in occasione di cambiamenti di mansioni o di introduzione di nuovi strumenti, rilevanti rispetto al trattamento dei dati personali;
- adozione di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari.

In pratica e in generale occorre:

- nominare le figure previste dal Codice in materia di protezione dei dati personali (titolare, responsabile, incaricati);
- attivare una serie di **password** con determinate caratteristiche e con particolari modalità di gestione;
- adottare programmi volti a prevenire la vulnerabilità di strumenti elettronici e che tali programmi siano aggiornati con cadenza almeno annuale (antivirus);
- effettuare il salvataggio dei dati con frequenza almeno settimanale;



- redigere il documento programmatico di sicurezza che deve contenere informazioni riguardo a:
 - l'elenco dei trattamenti dei dati,
 - la distribuzione dei compiti e delle responsabilità (nomi di coloro che trattano i dati)
 - l'analisi dei rischi che incombono sui dati,
 - le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione dei locali in cui vengono custoditi i dati stessi (in certi casi armadi chiusi a chiave),
 - la previsione della formazione degli incaricati (circa anche le copie di sicurezza)
 - la descrizione dei criteri da adottare per garantire l'adozione delle misure di sicurezza nel caso in cui sia necessario affidare a terzi, estranei alla struttura, i dati personali,
 - l'individuazione di criteri da adottare per la separazione di dati idonei a rivelare lo stato di salute e la vita sessuale dagli altri dati personali.

Il 31 dicembre 2004 è il termine per la predisposizione del documento programmatico sulla sicurezza. Il 31 marzo 2005 è il termine per l'adozione delle misure per coloro che non potranno, per certificate ragioni, farlo entro lo stesso 31 dicembre 2004.

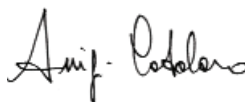
Anche la Direzione generale dell'Ufficio scolastico regionale per il Piemonte ha predisposto in data 16/07/2004 e adottato con provvedimento prot. nr. 8004/P/A22 del 21/10/2004, il Documento Programmatico sulla Sicurezza (DPS). In esso ha operato la sintesi descrittiva del complesso di attività poste in essere per la messa in sicurezza del Sistema Informativo.

Questo Ufficio vuole condividere con tutte le Istituzioni scolastiche della Regione la sua esperienza e, grazie al lavoro del gruppo del progetto SisCAS, ha messo a disposizione del materiale che possa guidare le istituzioni scolastiche nella stesura del DPS e un fac-simile dello stesso che, integrato con un'opportuna mappatura della particolare situazione hardware e software di ciascuna istituzione scolastica, consenta di redigere agevolmente il DPS.

Tutto questo materiale è prelevabile dal sito www.siscas.net/dps a partire da **martedì 26 ottobre 2004**.

Qualora si riscontrassero difficoltà, siete pregati di segnalarlo alla casella di posta elettronica dLgs196@siscas.net. Sulla base delle segnalazioni pervenute saranno attivate ulteriori azioni di supporto.

IL DIRETTORE GENERALE
Luigi CATALANO



NORMATIVA NAZIONALE

- **Decreto legge n. 266 del 9 novembre 2004** (in attesa di conversione)
proroga o differimento di termini previsti da disposizioni legislative
- **Decreto legislativo n. 196 del 30 giugno 2003**
Codice in materia di protezione dei dati personali
 - allegato A1
 - allegato A2
 - allegato A3
 - allegato B
- **Legge n. 325 del 3 novembre 2000**
Disposizioni inerenti all'adozione delle misure minime di sicurezza nel trattamento dei dati personali previste dall'articolo 15 della legge n. 675 del 31 dicembre 1996
- **Decreto del Presidente della Repubblica n. 318 del 28 luglio 1999**
Regolamento recante norme per l'individuazione delle misure minime di sicurezza per il trattamento dei dati personali, a norma dell'articolo 15, comma 2, della legge n. 675 del 31 dicembre 1996
- **Decreto legislativo n. 282 del 30 luglio 1999**
Disposizioni per garantire la riservatezza dei dati personali in ambito sanitario
- **Decreto legislativo n. 281 del 30 luglio 1999**
Disposizioni in materia di trattamento dei dati personali per finalità storiche, statistiche e di ricerca scientifica
- **Decreto legislativo n. 135 del 11 maggio 1999**
Disposizioni integrative della legge 31 dicembre 1996, n. 675, sul trattamento di dati sensibili da parte dei soggetti pubblici (con aggiornamenti)
- **Decreto legislativo n. 51 del 26 febbraio 1999**
Disposizioni integrative e correttive della legge 31 dicembre 1996, n. 675, concernenti il personale dell'Ufficio del Garante per la protezione dei dati personali



- **Decreto legislativo n. 389 del 6 novembre 1998**
Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici
- **Decreto legislativo n. 171 del 13 maggio 1998**
Disposizioni in materia di tutela della vita privata nel settore delle telecomunicazioni, in attuazione della direttiva 97/66/CE del Parlamento europeo e del Consiglio, ed in tema di attività giornalistica (modificato dal D.L.vo 467/2001)
- **Decreto legislativo n. 135 del 8 maggio 1998**
Disposizioni in materia di trattamento di dati particolari da parte di soggetti pubblici
- **Decreto legislativo n. 255 del 28 luglio 1997**
Disposizioni integrative e correttive della Legge n. 675 del 31 dicembre 1996, in materia di notificazione dei trattamenti di dati personali, a norma dell'art. 1, comma 1, lettera f), Legge n. 676 del 31 dicembre 1996
- **Decreto Legislativo n. 123 del 9 maggio 1997**
Disposizioni correttive ed integrative della legge 31 dicembre 1996, n. 675 in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali
- **Legge n. 675 del 31 dicembre 1996**
Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali



Nelle pagine successive è presentato un fac-simile di documento programmatico sulla sicurezza strutturato in un esempio base, 6 allegati e modelli di lettere di incarico.

Non esiste un documento programmatico sulla sicurezza che valga in generale per tutte le situazioni. Ogni scuola deve pertanto strutturarli su dati di fatto reali che non è possibile prevedere in tutte le loro sfaccettature.

Il nostro intento è quello di proporre un esempio dal quale le scuole possano trarre utili elementi. Nel testo proposto le parti scritte in rosso sono da completare, integrare o modificare a cura del responsabile della sicurezza informatica dell'istituzione scolastica che redige il documento. La redazione del documento risulterà facile e agevole solo dopo aver effettuato un'opportuna mappatura della struttura organizzativa e della situazione hardware e software dell'istituzione scolastica.

Tutti i modelli predisposti in questa sezione sono scaricabili in formato RTF nella sezione "compilazione DPS" del sito www.siscas.net/dps

COPERTINA DEL DPS

DENOMINAZIONE DELLA SCUOLA
INDIRIZZO

DISPOSIZIONI MINIME SULLA SICUREZZA **E** **DOCUMENTO PROGRAMMATICO SULLA SICUREZZA**

Il presente documento si compone di n. pagine (inclusa la presente)

LUOGO E DATA
Prot. nr.

Il responsabile della sicurezza
(NOME COGNOME)

(firma)



DENOMINAZIONE DELLA SCUOLA

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 dalla **SCUOLA...**, previsti dal D. L.vo 30/06/2003 n. 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 (vedere il [Quaderno n.7](#))

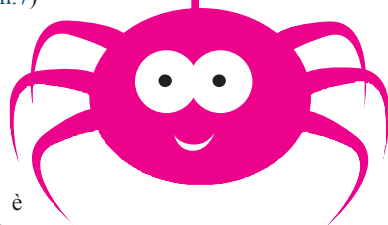
Articolo 2

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 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 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 (ISTITUZIONE SCOLASTICA) 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.

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:

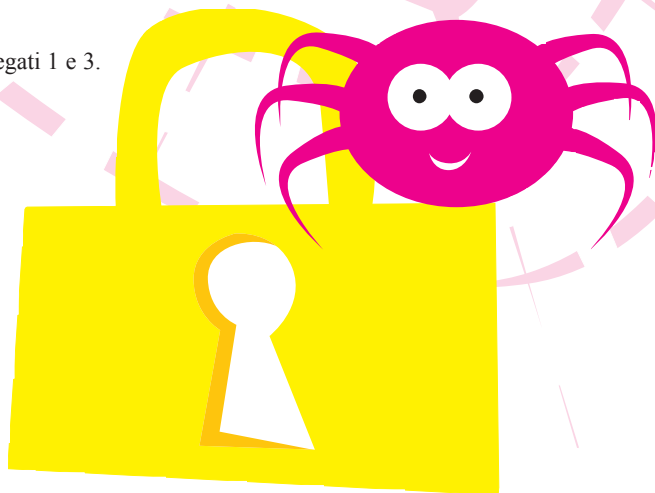
- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
 - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
 - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
 - DATI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



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)

Rischi	Deliberato	Accidentale	Ambientale
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		
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.

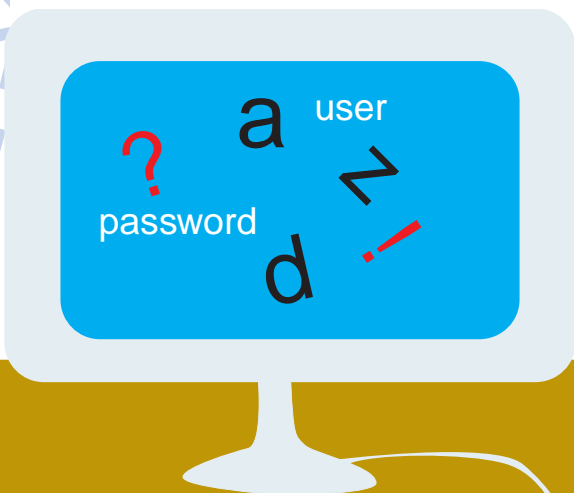
Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre, ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile di 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



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	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 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 della **SCUOLA.....**;
- 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 della SCUOLA**;
- 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

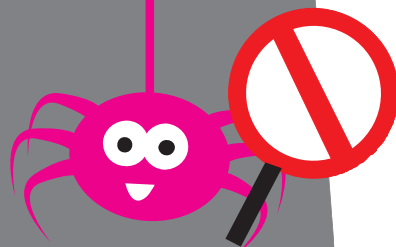
- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, 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.
- 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 della SCUOLA 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 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 n. 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.



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)
- Lettera di incarico per il trattamento dei dati
- Lettera di incarico per il responsabile del trattamento dati
- Lettera di incarico per il custode delle password
- Lettera di incarico per l'amministratore di sistema
- Lettera di incarico per il responsabile della sicurezza informatica
- Lettera di incarico di designazione dei componenti dell'unità organizzativa "docenti" ad incaricati del trattamento di dati personali

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)

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



DENOMINAZIONE DELLA SCUOLA

Tabella 1 - Elenco dei trattamenti dei dati

Descrizione sintetica del Trattamento		Natura dei dati trattati	Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati				

Descrizione sintetica: menzionare il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta (es. gestione del personale docente ed A.T.A., gestione collaboratori, gestione alunni, gestioni fornitori, ecc.) e delle categorie di persone cui i dati si riferiscono (alunni, famiglie, personale docente ed A.T.A., collaboratori, 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
 - 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, segreteria didattica, 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...).



Tabella 2 - Descrizione della struttura organizzativa della SCUOLA

Struttura	Trattamenti effettuati sulla struttura	Descrizione dei compiti e delle responsabilità della struttura
<i>Segreteria amministrativa</i>		
<i>Segreteria Didattica</i>		

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.).



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

Nome e cognome	Struttura di riferimento	Strumenti utilizzati	Responsabilità aggiuntive

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



DENOMINAZIONE DELLA SCUOLA

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;
- malfunzionamenti dovuti a sabotaggi, furti, intercettazioni (apparati di comunicazione).

MINACCE A CUI SONO SOTTOPOSTE LE RISORSE CONNESSE IN RETE

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

- all'utilizzo della LAN/Intranet (interne);
- 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).

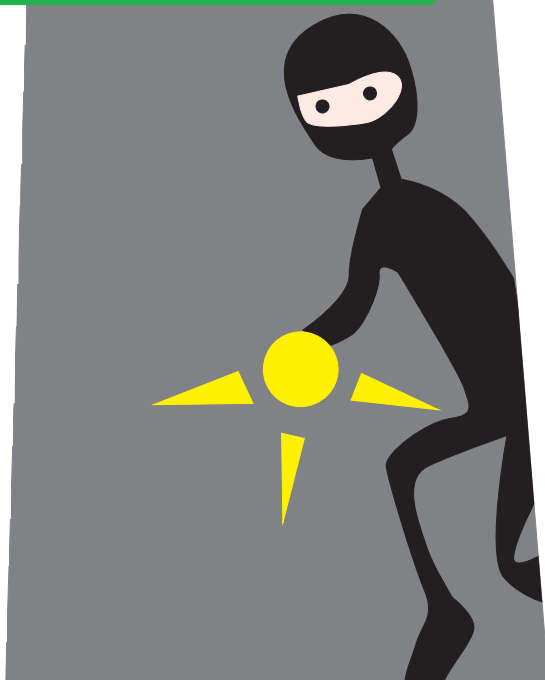
In dettaglio si evidenziano le seguenti tecniche:

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, ecc.).



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

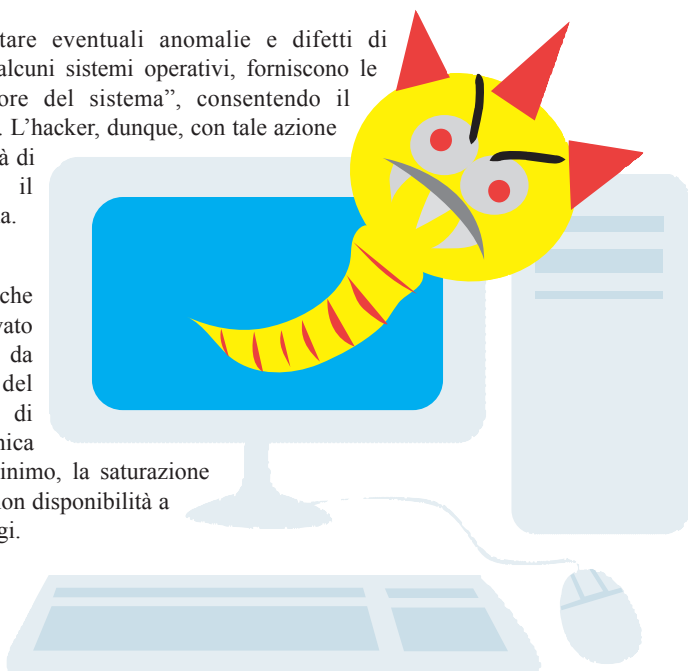
Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo.

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

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 inconsiamente 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.

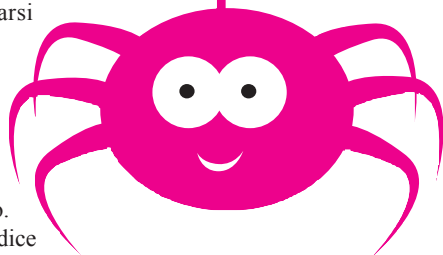
DOS (DENIAL OF SERVICE)

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 della



SCUOLA...; tali programmi non sono in nessun caso utilizzati su reti esterne a quella della scuola

La lettura in chiaro dei pacchetti in transito può solo essere autorizzata dall’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.



DENOMINAZIONE DELLA SCUOLA

Tabella 1 - Connettività internet

Connettività	Apparecchiature di comunicazione	Provider

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 (MIUR, RUPAR, altro).

Tabella 2 - Descrizione Personal Computer¹

Identificativo del PC	Tipo PC	Sistema operativo	Software utilizzato	rete

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. SISSI, OFFICE, STAROFFICE, ecc...).

Rete: indicare se il PC è connesso alla rete.

MISURE DI CARATTERE ELETTRONICO/INFORMATICO

Le misure di carattere elettronico/informativo² adottate sono:

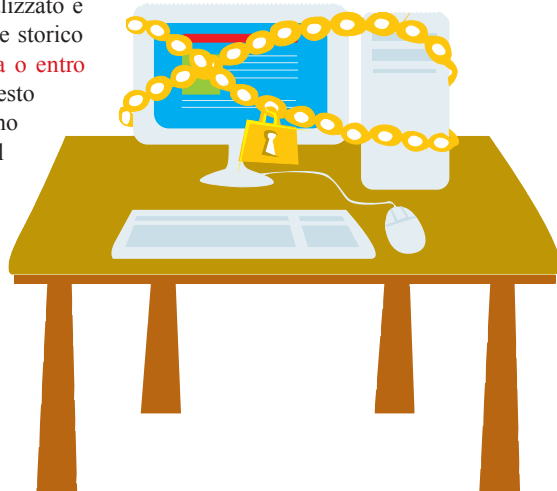
- utilizzo di server con configurazioni di ridondanza (indicare se la misura è attiva o entro quando sarà adottata);

1) I PC descritti in questa tabella **non** prendono in considerazione quelli presenti nei laboratori didattici

2) Le misure di carattere elettronico/informativo sono quelle in grado di segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, di gestire le copie di salvataggio dei dati e degli applicativi, di assicurare l'integrità dei dati, di proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi.



- presenza di gruppi di continuità elettrica per il server (indicare se la misura è attiva o entro quando sarà adottata);
- 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;
- 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);
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000 e XP, di seguito specificate (indicare se la misura è attiva o entro quando sarà adottata);
- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows 9x e Windows Me;
- installazione di un sistema antivirus su tutti 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 (indicare se la misura è attiva e quale prodotto è utilizzato o entro quando sarà adottata);
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate;
- separazione della rete locale delle segreterie da quella dei laboratori didattici (indicare se la misura è attiva o entro quando sarà adottata).



REGOLE PER LA GESTIONE DELLE PASSWORD³

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.

³ La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.



L'userid 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 userid e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

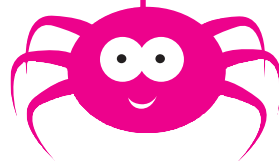
Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.

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 otto caratteri alfanumerici e non deve essere facilmente individuabile;
 - **deve contenere almeno un carattere alfabetico ed uno numerico;**
 - **non deve contenere più di due caratteri identici consecutivi;**
 - **non deve contenere lo userid 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.



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:

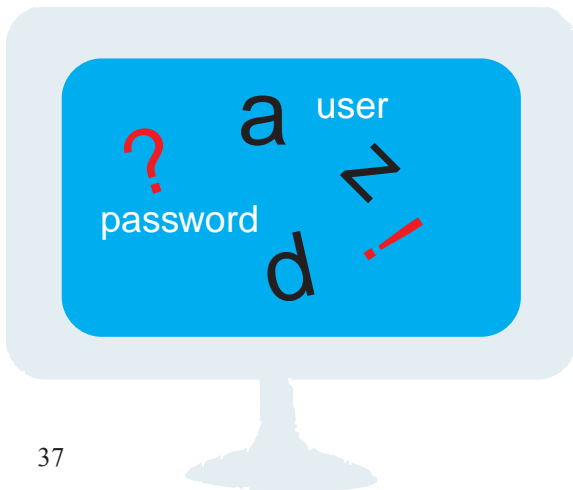
- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su ...**(indicare il dispositivo, CD, cassetta, ecc...)** sono conservate in ...**(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 controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

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

Il fax si trova in locale ad accesso controllato **(specificare dove)** e l'utilizzo è consentito unicamente agli incaricati del trattamento **(specificare chi)**.

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 dichiara 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 VIRUS⁴

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 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);

⁴ Le più recenti statistiche internazionali citano il virus informatico come la minaccia più ricorrente ed efficace



- 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:

1. formattare l'Hard Disk, definire le partizioni e reinstallare il Sistema Operativo (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
2. installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
3. reinstallare i programmi applicativi a partire dai supporti originali;
4. 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;
5. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
6. ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

INCIDENT RESPONSE E RIPRISTINO⁵

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.

⁵ Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni.



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 riacceso*;
4. documentare tutte le operazioni.

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

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

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

6) È indispensabile che per una eventuale indagine venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino affrettato del sistema potrebbe alterare le prove dell'incidente.



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	<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. Department of Energy)



DENOMINAZIONE DELLA SCUOLA

Articolo 1

OGGETTO E AMBITO DI APPLICAZIONE

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

La rete della **SCUOLA** è connessa alla rete Internet.

Articolo 2

PRINCIPI GENERALI - DIRITTI E RESPONSABILITÀ

La **SCUOLA** 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. È 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.



Articolo 3 ABUSI E ATTIVITÀ VIETATE

È vietato ogni tipo di abuso¹. 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 della **SCUOLA**;
- 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 a quella della **SCUOLA**;
- 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;
- 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 della **SCUOLA** 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;

¹ Si intende con abuso qualsiasi violazione del presente regolamento e di altre norme civili, penali e amministrative che disciplinano le attività e i servizi svolti sulla rete e di condotta personale.



- 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.

Articolo 4 ATTIVITÀ CONSENTITE

È consentito all'amministratore di sistema:

- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password 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.

Articolo 5 SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

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

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

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

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

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



Articolo 6 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.

Articolo 7 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 della **SCUOLA**



DENOMINAZIONE DELLA SCUOLA

L'utilizzo del proxy riguarda le misure procedurali relative all'identificazione e all'autenticazione degli utenti, le regole di utilizzo delle risorse hardware e software, le norme comportamentali e le responsabilità di ciascuno. Rientrano in questo aspetto le norme di comportamento interno per limitare l'uso privato di e-mail o Internet, in quanto i controlli sono possibili solo a determinate condizioni e con l'accordo delle rappresentanze sindacali unitarie. Si ricorda che il D. L.vo 196/03 (Codice in materia di protezione dei dati personali) ribadisce quanto dettato dall'art. 4 dello Statuto dei Lavoratori, ovvero il "... divieto di utilizzo da parte del datore di lavoro di apparecchiature atte al controllo a distanza dell'attività del lavoratore, salvo che esigenze organizzative, produttive o di sicurezza non abbiano determinato, previo accordo con le rappresentanze sindacali, la lecita introduzione in azienda". D'altro canto la consultazione di siti web da parte del lavoratore o l'utilizzo di posta elettronica durante il normale orario di lavoro non è consentita quando tale attività non sia pertinente con le mansioni affidate, come l'art. 1024 del codice civile prevede nel principio generale di diligenza del lavoratore. Per trovare un punto di equilibrio tra i diritti del lavoratore e della scuola è opportuno introdurre una policy trasparente e codificata con l'apporto dei lavoratori, dando anche la possibilità al datore di lavoro di prevedere meccanismi sanzionatori, sempre che la policy sia resa accessibile a tutti i lavoratori, come previsto dall'art. 7 dello Statuto dei Lavoratori. Sempre tra le politiche di sicurezza si può fare riferimento alle responsabilità civili e penali per i danni cagionati con il trattamento dei dati personali. A titolo di esempio si possono elencare:

1. la responsabilità civile disciplinata dall'art. 2050 del Codice Civile e art. 15 D.Lgs. 196/03 "chi cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto a risarcire il danno, a meno che non provi di aver adottato tutte le misure idonee per evitarlo";



2. la sanzione penale che colpisce chi, essendovi tenuto, omette di adottare le misure di sicurezza (art. 169 del D. L.vo 196/03), pari all'arresto fino a due anni o ad ammenda da 10mila a 50mila euro, ma con estinzione del reato in caso di regolarizzazione entro 6 mesi dall'accertamento del reato e pagamento di somma determinata dal Garante.

Le informazioni e le attività eseguite sulla rete informatica e telematica della **SCUOLA...** relative agli utilizzatori, sono registrate e conservate su file (registro elettronico delle attività o file di log).

Tali file possono essere soggetti ad indagini, nel rispetto di quanto sancito dal D. L.vo 30 giugno 2003, n. 196. Inoltre, il responsabile per la sicurezza può accedere ai file degli utilizzatori per proteggere l'integrità dei sistemi informatici.

Per il regolamento d'uso della rete (policy) vedere l'Allegato 4.



DENOMINAZIONE DELLA SCUOLA

Nell'esercitare attività di videosorveglianza, la **SCUOLA...** rispetta il principio di proporzionalità tra i mezzi impiegati ed i fini perseguiti, in particolare si precisa che:

- il trattamento dei dati avviene secondo correttezza e per scopi determinati, espliciti e legittimi;
- l'attività è svolta per la prevenzione di un pericolo concreto o di specifici reati, solo le autorità competenti sono legittimate ad accedere alle informazioni raccolte.

Inoltre l'attività di videosorveglianza è esercitata osservando le seguenti indicazioni:

- sono fornite alle persone che possono essere riprese, indicazioni chiare, anche se sintetiche, circa la presenza di impianti di videosorveglianza;
- è scrupolosamente rispettato il divieto di controllo a distanza dei lavoratori;
- sono raccolti i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo di visuale delle riprese, evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti;
- il periodo di conservazione dei dati è limitato allo stretto necessario e non eccede mai i **cinque giorni**;
- la conservazione dei dati oltre il termine previsto alla lettera d), è possibile solo in relazioni al verificarsi di illeciti o quando siano in corso indagini giudiziarie;
- i dati raccolti per fini determinati non sono utilizzati per finalità diverse o ulteriori, fatte salve le esigenze di polizia o di giustizia e non sono diffusi o comunicati a terzi.



Prot. n.

LUOGO E DATA

Oggetto: Lettera di incarico al trattamento dei dati.

Il sottoscritto (nome cognome del responsabile del trattamento) responsabile del trattamento dei dati della SCUOLA...., sito in (indicare VIA - CITTÀ) conferisce al Sig. (nome cognome dell'incaricato) nato a (CITTÀ) il (DATA) l'incarico di compiere le operazioni di trattamento dei dati sotto elencate, nell'ambito delle funzioni di (indicare le mansioni) che è chiamato a svolgere, con l'avvertimento che dovrà operare osservando le direttive del titolare /responsabile.

A tal fine vengono fornite informazioni ed istruzioni per l'assolvimento del compito assegnato:

- il trattamento dei dati deve essere effettuato in modo lecito e corretto;
- i dati personali devono essere raccolti e registrati unicamente per finalità inerenti l'attività svolta;
- è necessaria la verifica costante dei dati ed il loro aggiornamento;
- è necessaria la verifica costante della completezza e pertinenza dei dati trattati;
- devono essere rispettate le misure di sicurezza predisposte dal titolare/responsabile riportate nel documento programmatico sulla sicurezza;
- in ogni operazione del trattamento deve essere garantita la massima riservatezza ed in particolare:
 - a) divieto di comunicazione e/o diffusione dei dati senza la preventiva autorizzazione del titolare/responsabile;
 - b) l'accesso ai dati dovrà essere limitato all'espletamento delle proprie mansioni ed esclusivamente negli orari di lavoro;
 - c) la fase di raccolta del consenso dovrà essere preceduta dalla informativa ed il consenso al trattamento degli interessati rilasciato in forma scritta;
- in caso di interruzione, anche temporanea, del lavoro verificare che i dati trattati non siano accessibili a terzi non autorizzati;
- le proprie credenziali di autenticazione devono essere riservate;
- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive del responsabile del trattamento dei dati; non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati sensibili e non;
- raccogliere, registrare e conservare i dati presenti negli atti e documenti contenuti nei fascicoli di studio e nei supporti informatici avendo cura che l'accesso ad essi sia possibile solo ai soggetti autorizzati;

- eseguire qualsiasi altra operazione di trattamento nei limiti delle proprie mansioni e nel rispetto delle norme di legge;
- qualsiasi altra informazione può essere fornita dal Titolare che provvede anche alla formazione.

Operazioni di trattamento dei dati cui può accedere il Sig. (nome cognome dell'incaricato):
(elenco delle operazioni)

Gli obblighi relativi alla riservatezza, alla comunicazione ed alla diffusione dovranno essere osservati anche in seguito a modifica dell'incarico e/o cessazione del rapporto di lavoro.

Per ogni altra misura ed istruzione qui non prevista ci si richiama al Documento Programmatico sulla Sicurezza.

Per accettazione dell'incarico
(NOME COGNOME)

(firma)

Il titolare del trattamento
(NOME COGNOME)

(firma)



Lettera di incarico

Prot. n.

LUOGO E DATA

Oggetto: Incarico di responsabile del trattamento dati.

Il sottoscritto (**nome cognome del titolare**), non in proprio, ma in qualità di rappresentante legale della **SCUOLA.....**, titolare del trattamento dei dati ai sensi del D. L.vo n. 196 del 30/06/2003, conformemente a quanto stabilito nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", **affida** al Sig. (**nome cognome del responsabile**) l'**incarico** di responsabile del trattamento dei dati con i seguenti compiti:

- promuovere lo sviluppo, la realizzazione ed il mantenimento del programma di sicurezza e vigilare sul rispetto delle norme indicate nel Documento Programmatico sulla Sicurezza;
- assegnare i trattamenti agli incaricati;
- assegnare le responsabilità per le aree ad accesso controllato;
- assegnare le responsabilità per le procedure di copia (backup);
- vigilare sul rispetto delle norme indicate nel Documento programmatico sulla sicurezza;
- informare il titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti;
- promuovere lo svolgimento di un continuo programma di addestramento degli incaricati del trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza;
- collaborare con il responsabile della sicurezza informatica;
- collaborare con l'amministratore di sistema.

Il responsabile testé incaricato dichiara di essere a conoscenza di quanto stabilito dal D. L.vo n. 196 del 30/06/2003 ed in particolare di quanto indicato nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme descritte nel Documento Programmatico sulla Sicurezza, in relazione ai compiti sopra indicati.

Per accettazione dell'incarico
Il responsabile del trattamento
(**NOME COGNOME**)

(firma)

Il titolare del trattamento
(**NOME COGNOME**)

(firma)



Lettera di incarico

Prot. n.

LUOGO E DATA

Oggetto: Incarico custode delle password

Il sottoscritto (**nome cognome del titolare**), non in proprio, ma in qualità di rappresentante legale della **SCUOLA....** titolare del trattamento dei dati ai sensi del D. L.vo n. 196 del 30/06/2003, conformemente a quanto stabilito nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", **affida** al Sig. (**nome cognome del custode**) l'**incarico** di custode delle password con i seguenti compiti:

- predisporre, per ogni incaricato del trattamento (qualora nominato) e per ogni Banca Dati, una busta sulla quale è indicato lo User-Id utilizzato e al cui interno è contenuta la Password usata per accedere alla Banca Dati;
- revocare tutte le password non utilizzate per un periodo superiore a 6 mesi;
- revocare tempestivamente tutte le password assegnate a soggetti che su comunicazione scritta del responsabile del trattamento non sono più autorizzati ad accedere ai dati;
- gestione delle buste contenenti le password degli incaricati del trattamento e conservarle in un luogo sicuro e protetto.

Il custode delle password testè incaricato dichiara di essere a conoscenza di quanto stabilito dal D. L.vo n. 196 del 30/06/2003 ed in particolare da quanto indicato nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme in esso descritte, in relazione ai compiti sopra indicati.

Per accettazione dell'incarico
Il custode delle password
(NOME COGNOME)

(firma)

Il titolare del trattamento
(NOME COGNOME)

(firma)



Lettera di incarico

Prot. n.

LUOGO E DATA

Oggetto: Incarico di amministratore di sistema

Il sottoscritto (**nome cognome del titolare**), non in proprio, ma in qualità di rappresentante legale della **SCUOLA.....**, titolare del trattamento dei dati ai sensi del D. L.vo n. 196 del 30/06/2003, conformemente a quanto stabilito nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", **affida** al Sig. (**nome cognome dell'amministratore**) l'**incarico** di amministratore di sistema con i seguenti compiti:

- sovrintendere al funzionamento della rete, comprese le apparecchiature di protezione (firewall, filtri);
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- effettuare interventi di manutenzione hardware e software su sistemi operativi e applicativi;
- sovrintendere all'operato di eventuali tecnici esterni all'amministrazione;
- fare in modo che sia prevista la disattivazione dei codici identificativi personali (user-id), in caso di perdita della qualità che consentiva all'incaricato l'accesso al personal computer, oppure nel caso di mancato utilizzo del codice per oltre sei mesi;
- gestire le password di root o di amministratore di sistema
- collaborare con il responsabile del trattamento dei dati personali;
- collaborare con il custode delle password;
- informare il responsabile della sicurezza informatica sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.

L'amministratore testé incaricato dichiara di essere a conoscenza di quanto stabilito dal D. L.vo n. 196 del 30/06/2003 ed in particolare di quanto indicato nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme descritte nel Documento Programmatico sulla Sicurezza, in relazione ai compiti sopra indicati.

Per accettazione dell'incarico
L'amministratore del sistema
(NOME COGNOME)

(firma)

Il titolare del trattamento
(NOME COGNOME)

(firma)



Lettera di incarico

Prot. n.

LUOGO E DATA

Oggetto: Incarico di responsabile della sicurezza informatica.

Il sottoscritto (**nome cognome del titolare**), non in proprio, ma in qualità di rappresentante legale della **SCUOLA.....**, titolare del trattamento dei dati ai sensi del D. L.vo n. 196 del 30/06/2003, conformemente a quanto stabilito nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza", **affida** al Sig. (**nome cognome del responsabile**) l'**incarico** di responsabile della sicurezza informatica con i seguenti compiti:

- definire le misure di sicurezza informatica da adottare e predisporre l'informativa per l'amministratore del sistema e per il responsabile del trattamento dei dati;
- collaborare con il responsabile del trattamento dei dati personali per definire il piano di formazione;
- informare il titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti.

Il Responsabile testé incaricato dichiara di essere a conoscenza di quanto stabilito dal D. L.vo n. 196 del 30/06/2003 ed in particolare di quanto indicato nell'allegato B "Disciplinare tecnico in materia di misure minime di sicurezza" e si impegna ad adottare tutte le misure necessarie all'attuazione delle norme descritte nel Documento Programmatico sulla Sicurezza, in relazione ai compiti sopra indicati.

Per accettazione dell'incarico
Il responsabile della sicurezza
(NOME COGNOME)

(firma)

Il titolare del trattamento
(NOME COGNOME)

(firma)



Prot. n.

LUOGO E DATA

Oggetto: incarico per il trattamento dei dati personali da parte dei componenti dell'unità organizzativa "docenti"

Il dirigente scolastico/il responsabile del trattamento dei dati

Visto:

il D. L.vo 196/2003 "Codice in materia di protezione dei dati personali", che d'ora in poi nel presente documento sarà richiamato semplicemente come "Codice";

Premesso che:

- ai sensi dell'art. 28 del Codice nel presente atto, Titolare dei dati personali trattati da parte di questa scuola è la scuola stessa, di cui il sottoscritto è Legale Rappresentante pro-tempore;
- il titolare ha (non ha) applicato l'art. 29 del Codice che consentiva la facoltà di nominare uno o più responsabili di tutti o parte dei trattamenti e che pertanto è stato nominato il Sig. (nome cognome del responsabile);
- l'art. 30 del Codice impone di nominare gli incaricati del trattamento dei dati;
- l'art. 33 impone di adottare le misure di sicurezza disposte dal Codice e almeno le misure minime individuate dall'allegato B del Codice stesso;

Considerato che:

- occorre definire le misure minime di sicurezza per l'attività di ciascuna unità organizzativa nel trattamento di dati personali e per l'esecuzione di procedimenti amministrativi e individuare gli Incaricati
- la nomina a incaricato non implica l'attribuzione di funzioni ulteriori rispetto a quelle già assegnate bensì soltanto ricevere un'autorizzazione a trattare dati personali e istruzioni sulle modalità cui attenersi nel trattamento
- l'articolazione organizzativa della scuola è fondata su 5 unità: collaboratori del Dirigente Scolastico, personale docente (compresi docenti esterni ufficialmente incaricati di esami o altre funzioni presso la scuola), personale di segreteria, personale ausiliario (Collaboratori scolastici) e membri (anche esterni alla scuola) degli Organi Collegiali

determina

1. di **designare l'unità organizzativa "docenti"** quale **incaricata** al trattamento dei seguenti dati personali elencati nell'Allegato 1 - Elenco dei trattamenti (che viene unito a questa determinazione):
 - T1 - Alunni - Dati personali trattati da Docenti (elencare i dati oggetto del trattamento da parte dei docenti);
2. che **anche docenti esterni** incaricati ufficialmente di funzioni nella scuola (esami, corsi, concorsi e attività integrative) entrino a pieno titolo in questa categoria;
3. di dare atto che ogni dipendente che cessa di far parte di questa unità organizzativa cessa

¹ L'unità organizzativa "docenti" comprende: docenti, assistenti alla didattica, insegnanti tecnico-pratici, educatori e docenti di sostegno



automaticamente dalla funzione di Incaricato, che ogni nuovo dipendente che entra a far parte di questa unità organizzativa assume automaticamente la funzione di incaricato, che in un determinato momento l'elenco degli incaricati appartenenti a questa categoria corrisponde all'elenco dei dipendenti validamente in servizio che ne fanno parte;

4. di autorizzare questa categoria di incaricati a trattare tutti i dati personali con cui entrino comunque in contatto nell'ambito dell'espletamento dell'attività di loro competenza e in particolare di poter consultare il fascicolo personale degli alunni e qualunque documento necessario per l'attività istituzionale;
5. di autorizzare l'unità organizzativa "docenti" a trattare i dati sensibili e giudiziari con cui vengano a contatto durante l'attività di loro competenza nell'ambito della scuola;
6. di indicare per l'unità organizzativa "docenti" quali misure di sicurezza da applicare tassativamente nel trattamento dei dati personali in genere, nella gestione di banche dati cartacee, le istruzioni operative riportate negli allegati 1 - 2 - 3 - 4 - 5 - 6, nella parte a loro dedicata e che fanno parte integrante del presente documento;
7. fermi restando obblighi e responsabilità civili e penali dei dipendenti pubblici nell'ambito delle attività d'ufficio, di disporre sotto vincolo disciplinare l'obbligo tassativo di attenersi alle suddette istruzioni per tutti i dipendenti facenti parte dell'unità organizzativa "Docenti";
8. di mettere a disposizione copia del D. L.vo 196/2003 ed altri materiali informativi;
9. di organizzare apposite riunioni esplicative e formative;
10. di mettere a disposizione, non appena redatto, il Documento Programmatico sulla Sicurezza;
11. di consegnare, all'atto dell'assunzione in servizio, a ogni nuovo componente anche temporaneo dell'unità organizzativa in oggetto copia della presente determina e i relativi allegati e di provvedere affinché riceva un'adeguata formazione individuale;
12. **di impartire le seguenti istruzioni generali:**
 - il responsabile e gli incaricati devono attenersi rigorosamente a tutte le regole dettate dal D. L.vo 196/2003 e in particolare hanno l'obbligo di mantenere in ogni caso il dovuto riserbo per le informazioni delle quali si sia venuti a conoscenza nel corso dell'incarico, anche quando sia venuto meno l'incarico stesso (art. 326 del codice penale e art. 28 della legge 241/90);
 - ai sensi dell'art. 30 del Codice gli incaricati del trattamento devono operare sotto la diretta autorità del titolare (o del responsabile, se nominato) e devono elaborare i dati personali ai quali hanno accesso attenendosi alle istruzioni impartite.
 - **finalità del trattamento:**
ai sensi dell'art. 18 del Codice in materia di protezione dei dati personali, il trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali;
 - **modalità di trattamento dei dati:**
il trattamento può essere effettuato **manualmente**, mediante **strumenti informatici, telematici o altri supporti**. Ai sensi dell'art. 11 del Codice, il trattamento deve



applicare il principio di **pertinenza e non eccedenza** rispetto alle finalità del trattamento medesimo, pertanto è consentita l'acquisizione dei soli dati personali strettamente indispensabili per adempiere alle finalità richieste dall'interessato. Si ricorda che ogni acquisizione di dati deve essere preceduta dall'apposita informativa all'interessato di cui all'art. 13 e 22, avendo cura nel caso di documenti ritenuti potenzialmente classificabili come sensibili o giudiziari di fare espresso riferimento alla normativa che prevede gli obblighi o i compiti in base alla quale è effettuato il trattamento;

- i dati devono essere trattati in modo **lecito e secondo correttezza**, devono essere **esatti ed aggiornati**;
- è vietata all'incaricato qualsiasi forma di diffusione e comunicazione dei dati personali trattati che non sia funzionale allo svolgimento dei compiti affidati;
- per il trattamento devono essere seguite le norme di legge in materia di tutela della riservatezza dei dati personali e devono essere applicate le misure di protezione previste dal titolare;
- **categorie di soggetti ai quali i dati possono essere comunicati:**
ai sensi dell'articolo 19 del codice la comunicazione da parte della scuola ad altri soggetti pubblici è ammessa quando è prevista da una norma di legge o di regolamento. In mancanza di tale norma la comunicazione è ammessa previa comunicazione al Garante e attesa del diniego o del silenzio-assenso dopo 45 giorni. La comunicazione da parte della scuola a privati o a enti pubblici economici e la diffusione sono ammesse unicamente quando sono previste da una norma di legge o di regolamento;
- **modalità di trattamento dei dati sensibili/giudiziari:**
ferma restando l'applicazione delle disposizioni vigenti in materia di trattamento dei dati sensibili e giudiziari e delle istruzioni impartite dal Titolare e dal Responsabile del trattamento, i documenti (anche tuttora in lavorazione e non definitivi) ed i supporti recanti dati sensibili o giudiziari devono essere conservati in elementi di arredo muniti di serratura e non devono essere lasciati incustoditi in assenza dell'incaricato;
- **trattamenti di dati inerenti la salute:**
i supporti ed i documenti recanti dati relativi alla salute e alle abitudini sessuali devono essere conservati separatamente in contenitori muniti di serratura.



LETTERA DI INCARICO

designazione dei componenti dell'unità organizzativa "docenti" ad incaricati del trattamento di dati personali

Il titolare del trattamento
(NOME COGNOME)

(firma)

Per presa visione

L'incaricato prof. (NOME COGNOME)

(firma)

L'incaricato prof. (NOME COGNOME)

(firma)

L'incaricato prof. (NOME COGNOME)

(firma)

L'incaricato prof. (NOME COGNOME)

(firma)

L'incaricato prof. (NOME COGNOME)

(firma)

L'incaricato prof. (NOME COGNOME)

(firma)

L'incaricato prof. (NOME COGNOME)

(firma)

L'incaricato prof. (NOME COGNOME)

(firma)

(elencare tutti i componenti la categoria e predisporre un ulteriore atto con pari data e protocollo da far firmare a quelli che arriveranno)



DENOMINAZIONE DELLA SCUOLA

Sig. _____
 Genitore dell'alunno _____
 Classe _____
 Plesso _____

Nell'ambito del rapporto instaurato o da instaurarsi con la nostra Scuola La informiamo che l'Istituzione Scolastica scrivente fa oggetto di trattamento, secondo la definizione di esso data dall'art. 4 comma 1 del D.L.vo 196/2003, dei dati personali che La riguardano, acquisiti con la domanda di iscrizione o con la dichiarazione presentata dall'Interessato che sottoscrive il presente modulo. Il trattamento dei dati è strettamente necessario per le finalità istituzionali della scuola e per il procedimento amministrativo richiesto, che altrimenti non potrebbe aver luogo. Il trattamento riguarderà unicamente le finalità richieste e quelle ad esse strettamente correlate, tutte rientranti tra quelle istituzionali relative all'istruzione, alla formazione degli allievi e alle attività amministrative, così come definite dalla normativa vigente e dai connessi regolamenti e leggi regionali, e per le quali vengono raccolti solo i dati strettamente necessari. Il trattamento potrà avere ad oggetto anche dati "sensibili" e "giudiziari", così come definiti dal D. L.vo 196/2003, quando ciò sia necessario per svolgere l'attività istituzionale. I dati personali definiti "sensibili" sono quelli "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". I dati giudiziari sono quelli "idonei a rivelare provvedimenti 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";

I dati saranno trattati con modalità manuali e con l'ausilio di strumenti elettronici o comunque automatizzati, secondo le modalità e le cautele previste dal predetto D. L.vo, e conservati per il tempo necessario all'espletamento delle attività amministrative e istituzionali riferibili alle predette finalità.

I soggetti che trattano i dati nell'ambito della scuola sono:

1. il Dirigente Scolastico, (**Il Responsabile del Trattamento - se nominato**), gli Incaricati del trattamento amministrativo, tutti vincolati all'assoluta riservatezza;
2. i docenti strettamente interessati (esclusivamente per i dati necessari alle attività didattiche, di valutazione, integrative e istituzionali);
3. i Collaboratori Scolastici e i componenti gli Organi Collegiali (Consigli di classe, Consiglio d'Istituto, Giunta Esecutiva) limitatamente ai dati strettamente necessari alla loro attività.

I dati personali potranno essere comunicati ad altri enti pubblici e privati soltanto nei casi previsti da leggi e regolamenti. I dati personali potranno essere comunicati, insieme ai necessari documenti originali, ad altra scuola al fine di consentire il trasferimento, nelle modalità previste dalle norme sull'Istruzione Pubblica.

Potranno essere diffusi esclusivamente nei casi previsti dalla legge.

¹L'informativa nei confronti di **ogni** interessato è obbligatoria. Una copia deve essere consegnata all'interessato, l'altra copia, firmata dello stesso per presa visione, deve essere conservata a cura dell'istituzione scolastica.

L'informativa deve essere specifica per le seguenti categorie di interessati: Famiglie - Dipendenti - Fornitori

In questa sezione proponiamo una bozza di informativa alle famiglie; per le altre indichiamo come riferimento il seguente URL:

http://www.siscas.net/dps/?Compilazione_del_DPS:informativa



Titolare del trattamento dei dati è la scuola stessa, che ha personalità giuridica autonoma ed è legalmente rappresentata dal Dirigente Scolastico in carica, elettivamente domiciliato presso la Scuola.

Responsabile del trattamento dei dati relativi ad alunni, dipendenti, collaboratori esterni e fornitori, affari generali e protocollo è il **DSGA** sig./sig.ra, elettivamente domiciliato presso la Scuola.

Per ulteriori informazione è possibile rivolgersi alla segreteria stessa (**indicare almeno un indirizzo e-mail**).

L'interessato cui i dati personali si riferiscono gode di una serie di diritti sanciti dall'art. 7 del D.Lgs 196/2003 che viene qui riportato:

"1. L'interessato ha diritto di ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile.

2. L'interessato ha diritto di ottenere l'indicazione:

- a) dell'origine dei dati personali;
- b) delle finalità e modalità del trattamento;
- c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici;
- d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato ai sensi dell'articolo 5, comma 2;
- e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

3. L'interessato ha diritto di ottenere:

- a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati;
- b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
- c) l'attestazione che le operazioni di cui alle lettere a, e b) sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccettuato il caso in cui tale adempimento si rivela impossibile o comporta un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

4. L'interessato ha diritto di opporsi, in tutto o in parte:

- a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;
- b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale."

Il/la sottoscritto/a (**nome e cognome del genitore**) genitore di (**nome e cognome dell'alunno**), dichiara di avere ricevuto l'informativa di cui all'art. 13 del D.Lgs 196/2003.

LUOGO E DATA

Per preva visione
(NOME COGNOME)

(firma leggibile)



DENOMINAZIONE DELLA SCUOLA

Gentile Signore,

facendo riferimento all'informativa che, in relazione ai rapporti in essere con la nostra scuola, Le abbiamo a suo tempo fornito e alla (indicare il tipo di attività: gita, visita di istruzione, ECDL,), le comunichiamo che per poter svolgere tale attività, pertinente alle attività istituzionali e/o connessa ad attività strumentali alle stesse, si rende necessario comunicare alcuni dati personali da Lei forniti a (indicare a quale **soggetto non istituzionale** saranno comunicati i dati)

Tali dati, diversi da quelli sensibili e giudiziari, e più precisamente (nome, cognome, luogo e data di nascita, indirizzo,) verranno trattati esclusivamente per la suddetta attività e non saranno comunicati ad altri soggetti, né saranno oggetto di diffusione.

Secondo le norme del D. L.vo 196/2003 tale trattamento sarà improntato ai principi di necessità, liceità, correttezza, finalità, proporzionalità, qualità dei dati (esatti, aggiornati, pertinenti, completi e non eccedenti) e alla tutela della sua riservatezza e dei suoi diritti così come indicato nella informativa che Le abbiamo fornito ai sensi dell'art. 13 del D. L.vo succitato e per i quali può esercitare i diritti previsti dall'art. 7.

L'eventuale rifiuto a prestare il consenso potrebbe comportare l'impossibilità di usufruire dell'attività come programmata.

Il/la sottoscritto/a (nome e cognome del genitore)
genitore di (nome e cognome dell'alunno) - classe
(indicare la classe),

acquisite le informazioni fornite dal titolare del trattamento ai sensi dell'art. 13 del D.L.vo 196/03, presta il suo consenso al trattamento dei dati personali per i fini su indicati

LUOGO E DATA

Per accettazione
(NOME COGNOME)

(firma)

1) Il trattamento dei dati personali in ambito pubblico è consentito per lo svolgimento delle funzioni istituzionali (art. 18 comma 2) e non è necessario il consenso dell'interessato (art. 18 comma 4), tuttavia per le attività di trattamento dei dati non istituzionali (ad esempio fornire alle aziende le indicazioni degli studenti diplomati) è necessario acquisire il consenso dell'interessato.



Il sottoscritto (nome e cognome dell'alunno)

Alunno della classe quinta Sez... (sezione e corso di studio) della **SCUOLA....**

- avendo conseguito il diploma conclusivo del corso di studi frequentato nel corrente anno scolastico presso l'Istituto;
- ricevuta l'informativa di cui all'art 13 D.L.vo 196/2003

Visto l'art. 96 del D.Lgs. n. 196/2003, qui riportato testualmente:

- "1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le scuole e gli istituti scolastici di istruzione secondaria, su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti scolastici, intermedi e finali, degli studenti e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle predette finalità e indicati nell'informativa resa agli interessati ai sensi dell'articolo 13. I dati possono essere successivamente trattati esclusivamente per le predette finalità.
2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati."

chiede

che sia applicata nei suoi confronti, fino ad una eventuale successiva diversa disposizione e/o revoca, la possibilità, prevista al comma 1 di tale articolo, di comunicare o diffondere, anche a privati e per via telematica, dati relativi ai propri esiti scolastici, intermedi e finali, e altri dati personali diversi da quelli sensibili o giudiziari, pertinenti in relazione alle finalità previste da tale disposizione normativa (nome, cognome, luogo e data di nascita, indirizzo, numero di telefono, fax, e-mail, nonché il possesso di titoli ed eventuali specializzazioni)

Dichiara che la presente funge anche da informativa per tali dati e finalità.

LUOGO E DATA

(NOME COGNOME)

(firma leggibile)



TERMINI RICORRENTI

AFFIDAMENTO DATI IN OUTSOURCING

affidamento della gestione dei dati a ditte o a persone esterne all'Ente per lo svolgimento di lavorazioni particolari.

BANCA DI DATI

qualsiasi complesso organizzato di dati ripartito in una o più unità dislocate in una o più posizioni.

BLOCCO

la conservazione di dati personali con sospensione temporanea di ogni altra operazione del trattamento.

CREDENZIALI DI AUTENTICAZIONE

dati e dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati utilizzati per l'autenticazione informatica.

DATI IDENTIFICATIVI

dati personali che permettono l'identificazione diretta dell'interessato

DATI ANONIMI

i dati che in origine, o a seguito del trattamento, non possono essere associati ad un interessato identificato o identificabile. Costituiscono la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza.

DATI PERSONALI

qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati od identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione ivi compreso un numero di identificazione personale. Costituiscono la classe di dati a rischio intermedio.

DATI SENSIBILI/GIUDIZIARI/SANITARI

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. Costituiscono la classe di dati ad alto rischio.

DIFFUSIONE

il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

GARANTE

l'autorità di cui all'articolo 153, istituita dalla legge 31 dicembre 1996, n. 675.

INCARICATI

le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile del trattamento. (Art. 4, Comma I, Lett. h D. L.vo 196/2003).



INTERESSATO

la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali.

MISURE MINIME DI SICUREZZA

il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'art. 31 (D. L.vo n. 196/2003).

PAROLA CHIAVE

componente di una credenziale associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica.

PROFILO DI AUTORIZZAZIONE

l'insieme delle informazioni, univocamente associate ad una persona, che consente di individuare a quali dati essa può accedere, nonché i trattamenti ad essa consentiti

RESPONSABILE DEL SISTEMA INFORMATIVO

il referente istituito dal D. L.vo 39/93 cui compete la pianificazione degli interventi di automazione, l'adozione delle cautele e delle misure di sicurezza.

RESPONSABILE PER IL TRATTAMENTO DEI DATI

la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo preposti dal titolare al trattamento di dati personali.

È designato dal titolare e deve garantire il rispetto delle norme in materia di trattamento dati e di sicurezza, i suoi compiti devono essere elencati per iscritto. La nomina del responsabile è facoltativa e non esonera da responsabilità il titolare.

SISTEMA DI AUTORIZZAZIONE

insieme di strumenti e procedure che abilitano l'accesso ai dati e alle modalità di trattamento degli stessi, in funzione del profilo del richiedente.

TITOLARE

la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza (nell'istituzione scolastica, la titolarità è esercitata dal dirigente scolastico).

TRATTAMENTO

qualsunque operazione o complesso di operazioni, svolti con o senza l'ausilio di mezzi elettronici o comunque automatizzati, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati.

UTENTE

qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico.

