



Prot. n° 1005/C14

Genova, 31 marzo 2010

DOCUMENTO PROGRAMMATICO

PER LA SICUREZZA

Decreto Legislativo 196 del 30 giugno 2003

INTRODUZIONE

Il presente documento definisce lo stato di attuazione nell'istituzione scolastica, SCUOLA STATALE SECONDARIA di PRIMO GRADO “DON MILANI - COLOMBO” – GENOVA, d'ora in poi ISTITUZIONE SCOLASTICA, per quanto disposto dal D.Leg. n° 196 del 30 giugno 2003, artt. da 33 a 36 e ALLEGATO B “DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA”.

Il contenuto di quanto segue si riferisce alla struttura organizzativa e funzionale dell'ISTITUZIONE SCOLASTICA che prevede il trattamento di dati effettuato, per le rispettive competenze, dal corpo docente, dal personale ATA.

Nell'affrontare e risolvere le varie problematiche riferite all'applicazione del D.Leg.vo n° 196/03 si è ritenuto opportuno quindi considerare, all'interno di uno stesso quadro organizzativo, in modo separato il trattamento dei dati operato dal personale docente e dal personale ATA.

I dati personali, comuni e sensibili, trattati da:

- **docenti** riguardano essenzialmente gli alunni;
- **dirigente scolastico, personale ATA (amministrativo e ausiliario)** riguardano sia gli alunni che il personale della scuola.

Il presente D.P.S. è strutturato nelle seguenti parti:

- A- ANALISI DELLA SITUAZIONE DELL'ISTITUZIONE SCOLASTICA
- B- MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE
- C- FORMAZIONE E ADEGUAMENTO DEL DOCUMENTO

A - Analisi della situazione DELL'ISTITUZIONE SCOLASTICA

1) Descrizione del Sistema Informatico

SEGRETERIA SEDE CENTRALE SCUOLA DON MILANI – COLOMBO

Salita Carbonara, 51 – 16125 GENOVA

In questa sezione vengono descritti gli elementi fondamentali del sistema informatico, individuando tutte le sue componenti, quali ad es.:

Hardware

- Reti locali ed altri sistemi di collegamento di terminali;

La segreteria scolastica, sita nella sede di Sal. Carbonara 51 - GENOVA, dispone di una rete locale composta da 1 SERVER e 6 PC CLIENT.

- Server e sistemi multiutenti presenti nell'ISTITUZIONE SCOLASTICA con i relativi sistemi operativi utilizzati;

Il SERVER ed i CLIENT sono in rete MICROSOFT WINDOWS.

I sistemi operativi installati sono:

SERVER → WINDOWS 2003 SERVER ITA

PC1 (PERSONALE 1) → WINDOWS XP PRO ITA

PC2 (PERSONALE 2) → WINDOWS XP PRO ITA

PC3 (DSGA) → WINDOWS XP PRO ITA

PC4 (DIDATTICA) → WINDOWS XP PRO ITA

PC5 (PROTOCOLLO) → WINDOWS XP PRO ITA

PC6 (PRESIDE) → WINDOWS XP PRO ITA

- Unità di accesso per gli utenti (terminali, personal computer, workstations, stampanti, telefax);

n. 1 TELEFAX

n. 6 PC CLIENT

n. 1 STAMPANTE DI RETE (Epson Aculaser C-1900) condivisa fra tutti gli utenti postaz. Segretaria DSGA

n. 1 STAMPANTE DI RETE (Epson Aculaser C-4100) condivisa fra tutti gli utenti

n. 1 STAMPANTE (Epson Aculaser C-1900) postaz. Preside

- Elaboratori portatili;

nessuno

- Collegamenti del sistema a rilevatori di presenze, od altri dispositivi di acquisizione dati (lettore ottico, scanner);

nessuno

- **Dispositivi di connessione verso l'esterno**, per singoli utenti o condivisi tra più utenti (modem,

router).

n. 1 ROUTER ADSL fornito fa FASTWEB – COMUNE DI GENOVA

n. 1 FIREWALL 3COM 3CR860-95 per protezione rete locale

N. 1 FIREWALL ZYWALL 2 PLUS Internet Security Appliance

Software

- Sistemi operativi utilizzati;

SERVER → WINDOWS 2003 SERVER ITA

PC1 (PERSONALE 1) → WINDOWS XP PRO ITA

PC2 (PERSONALE 2) → WINDOWS XP PRO ITA

PC3 (DSGA) → WINDOWS XP PRO ITA

PC4 (DIDATTICA) → WINDOWS XP PRO ITA

PC5 (PROTOCOLLO) → WINDOWS XP PRO ITA

PC6 (PRESIDE) → WINDOWS XP PRO ITA

- Applicazioni di tipo gestionale;

SISSI IN RETE

Software Server/Client per la gestione di segreteria scolastica.

Area Alunni, Personale, Retribuzioni, Biblioteca, Libri di testo, Magazzino, Gestione fiscale. Opensisi.

Base dati: CYBASE SQL 8.0.

Aggiornamenti di Sissi in Rete.

MIUR – SIDI

Sistema Integrato dell'Istruzione

UNICO ON LINE

Software per la compilazione dei modelli 770 – IRAP -DMA e l'invio dati al Ministero E.F.

Ambiente di sicurezza Entratel

INPS 2000

Software per il controllo dei Mod. EMENS – DM10 e invio dati

PRE 96

Software per trasmissione dati conguaglio retributivo al M.E.F.

SARE

Software per la comunicazione on-line dei contratti di lavoro alla Regione Liguria

- Applicazioni di office automation;

Microsoft Office 2003 (Word, Excel, Power point, Access, Outlook)

AVG Antivirus

- Software Didattico;

nessuno

- **Sistemi di posta elettronica e strumenti di navigazione in Internet;**

OUTLOOK EXPRESS
INTERNET EXPLORER

- Siti Internet interni o in hosting o housing presso provider;
nessuno

2) Analisi ed elenco dei dati personali

La sezione presenta le applicazioni esistenti (programmi di utilità), e sulla base delle informazioni gestite, determina se esse trattano, anche potenzialmente dati personali secondo quanto previsto dal codice sulla Privacy.

Particolare attenzione è posta riguardo all'utilizzo dei prodotti di office automation, data la libertà d'azione che tali prodotti concedono agli utenti sia riguardo al contenuto dei documenti generati, sia riguardo alla loro gestione (es. Salvataggio e backup).

Nella sezione sono individuate ed elencate, anche mediante ALLEGATO,

- le *banche dati informatiche* realizzate con le specifiche applicazioni software in uso all'ISTITUZIONE SCOLASTICA (ad es. Anagrafica Alunni/Docenti/Fornitori, ecc.)
 - gli archivi cartacei
- specificandone le finalità di trattamento.

In sintesi, le informazioni da riportare nella sezione sono:

- **per il trattamento con strumenti elettronici**
 - I server e/o i sistemi su cui sono archiviati i dati
 - Le applicazione utilizzate per il trattamento
 - Le finalità del trattamento
 - Presenza di dati sensibili o giudiziari
- **per il trattamento manuale (su supporto cartaceo, senza l'ausilio di strumenti elettronici)**
 - Dislocazione fisica degli archivi
 - Le finalità del trattamento
 - Presenza di dati sensibili o giudiziari.

Elenco dei trattamenti

Relativamente alla natura dei dati trattati, appare opportuno considerare i dati trattati dal personale dell'ISTITUZIONE SCOLASTICA nel loro insieme come dati sensibili, ai sensi dell'articolo 4 del decreto legislativo n 196 del 30 giugno 2003, c.1 lett.b,c,d.

Il trattamento dei dati da parte dei docenti (tenuta dei registri, modalità di compilazione dei documenti di valutazione, verbalizzazione etc.) è definito puntualmente da norme di legge o regolamentari.

VEDI ALLEGATO

3) Struttura organizzativa funzionale al trattamento dati e singole responsabilità

La sezione riporta gli elementi fondamentali della struttura organizzativa dell'ISTITUZIONE SCOLASTICA coinvolti nel trattamento dei dati personali, specificandone le singole responsabilità.

In particolare nella sezione vengono evidenziati:

- Il “titolare del trattamento” dei dati;
- Il/i “responsabile/i del trattamento” dati (se nominato/i in quanto facoltativo)
- Gli “incaricati del trattamento”
- Profili di autorizzazione individuati per singolo incaricato o per classi omogenee di incaricati (es. Docenti, Segreteria Didattica, Segreteria Amministrativa, ecc.)
- Il custode delle credenziali (amministratore del sistema informatico)
- Gli eventuali prestatori di servizi che trattano all'esterno dell'impresa dati per conto della stessa impresa (consulenti, professionisti, società di assistenza software, ...).

Il documento potrà contenere, in allegato,

- gli atti di nomina dei responsabili/incaricati,
- le istruzioni scritte comunicate agli incaricati (nominative o per classi omogenee) ed al custode delle credenziali.

Sono altresì specificate le responsabilità connesse alle mansioni da ciascuno ricoperte all'interno dell'ISTITUZIONE SCOLASTICA.

Il Titolare

Il Titolare è l'ISTITUZIONE SCOLASTICA, rappresentata dal Dirigente Scolastico (art. 28 D.L. N 196/2003).

Il Responsabile

Premessa: In base a quanto disposto dall'articolo 29 comma 2 del decreto legislativo n 196 del 30 giugno 2003, “ *Il responsabile se designato, deve essere nominato fra i soggetti che per esperienza capacità ed affidabilità, forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo della sicurezza*”.

Per la individuazione del responsabile, la cui nomina è facoltativa, esistono diverse possibilità:

- non viene nominato, ed il Dirigente Scolastico assume personalmente tutte le incombenze relative agli adempimenti previsti dal decreto legislativo n 196 del 30 giugno 2003 e provvedimenti collegati;
- viene nominato il Direttore dei Servizi Generali ed Amministrativi per i trattamenti dei dati che riguardano in modo specifico i servizi di segreteria mentre il Dirigente Scolastico si occupa direttamente del trattamento dei dati effettuato dai docenti.

Gli Incaricati

Il **DOCENTE** è da considerarsi, per la propria sfera di competenza, incaricato del trattamento come tale deve essere nominato mediante specifico atto che elenchi puntualmente:

- categorie dei dati cui può avere accesso;
- tipologia di trattamento e vincoli specifici applicabili alle varie tipologie di dati;
- istruzioni in merito ai soggetti cui i dati possono essere comunicati o diffusi.

Ogni **ASSISTENTE AMMINISTRATIVO** dovrà essere nominato incaricato del trattamento con specifico atto, in base ai compiti che assolve nell'ufficio.

I **COLLABORATORI SCOLASTICI**, qualora trattino anche saltuariamente dati personali, dovranno essere incaricati con specifico atto.

Le nomine saranno effettuate anche per il **personale supplente temporaneo, docente e ATA**, e, per quanto riguarda i trattamenti effettuati con strumenti elettronici, per il **personale esterno incaricato della manutenzione**.

Qualora l'ISTITUZIONE SCOLASTICA si dovesse avvalere per le pulizie, o per altri servizi, di imprese private e qualora i dipendenti di tali imprese, nell'ambito del servizio, avessero accesso ad aree contenenti archivi di dati personali, gli stessi dipendenti dovranno essere identificati e autorizzati dal RESPONSABILE.

L'Amministratore del Sistema Informatico

L'Amministratore di sistema garantisce la tutela ed il corretto uso dei sistemi informatici e delle banche-dati in essa contenuti.

A tal fine predispone un REGOLAMENTO INTERNO che deve essere disponibile a tutto il personale che opera nel LABORATORIO INFORMATICO e/o negli uffici dotati di sistemi informatici.

4) Analisi dei rischi possibili e dei danni conseguenti

Questa sezione rappresenta il nucleo fondamentale del documento, in quanto sulla base di questa valutazione l'ISTITUZIONE SCOLASTICA individua le specifiche azioni da intraprendere.

Si individuano ed elencano i possibili rischi cui è esposto il sistema informatico, quali ad es.:

- Alterazione/danneggiamento accidentale o dolosa del sistema, dei programmi e/o dati
- Diffusione/comunicazione non autorizzata sia accidentale che dolosa
- Danneggiamento delle risorse informatiche per disastri naturali (incendi...)
- Accessi non autorizzati
- Sottrazione di elaboratori, programmi, supporti o dati
- Intrusioni dall'esterno nel sistema

Si individuano altresì i tipi di danni arrecabili ai dati personali (fermo restando che l'adozione delle misure serve anche a garantire il know-how ed in genere il patrimonio informativo dell'ISTITUZIONE SCOLASTICA), quali ad es.:

- Distruzione dei dati
- Alterazione dei dati
- Trattamento/comunicazione/diffusione non autorizzata dei dati.

B – MISURE DI SICUREZZA adottate o da adottare

1) Procedure relative alle misure imposte dal Disciplinare tecnico

Premessa

Il disciplinare tecnico è l'allegato B al Codice della privacy.

Scopo della sezione è evidenziare in quale maniera le misure minime di sicurezza vengono realizzate nella realtà tecnologica ed organizzativa dell'ISTITUZIONE SCOLASTICA.

In particolare sono evidenziate:

Misure minime per i trattamenti informatici

- Definizione delle credenziali di autenticazione, individuate tra le seguenti tipologie:
 1. Codice identificativo, più parola chiave (*login e password*)
 2. Dispositivo di autenticazione (*smart card e simili*), più eventuale parola chiave
- Individuazione del custode delle credenziali (*generalmente è l'amministratore di sistema*)
- Modalità di attivazione, variazione e gestione delle credenziali
- Criteri di definizione dei profili di autorizzazione
- Attribuzione, revoca ed aggiornamento dei profili di autorizzazione
- Criteri di adozione, utilizzo e di aggiornamento dei sistemi antivirus (*l'aggiornamento del software antivirus deve essere fatto con cadenza almeno bisettimanale*).
- Criteri di adozione, utilizzo e di aggiornamento dei sistemi di antintrusione (*firewall*)
- Verifica dell'efficacia ed efficienza dei sistemi antivirus e antintrusione (*verifica annuale*).

NOTA su CODICE IDENTIFICATIVO (rif. DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA: Trattamento con strumenti elettronici – Sistema di autenticazione informatica).

- Deve essere unico, uno per ogni operatore. Non può essere assegnato ad altri incaricati.
- Il codice identificativo deve essere eliminato dopo sei mesi di non utilizzo
- La password è composta da almeno otto caratteri e non deve essere riconducibile all'utente
- La password è sostituita dall'incaricato al primo utilizzo e cambiata ogni sei mesi in caso di trattamento di dati personali, ogni tre mesi in caso di trattamento di dati personali sensibili.
- La password è strettamente personale e non deve essere comunicata e/o diffusa.
- Per garantire la continuità in caso di assenza della persona, l'ISTITUZIONE SCOLASTICA può prevedere che le password vengano consegnate in busta chiusa al TITOLARE che, in situazioni di emergenza, potrà utilizzarla. Alla ripresa dell'attività, l'interessato dovrà essere immediatamente avvisato e dovrà provvedere al cambio della password.

Misure minime per i trattamenti cartacei

- Procedure e modalità per l'organizzazione degli archivi cartacei ad accesso autorizzato;
- Modalità di custodia dei dati particolari durante l'utilizzo;
- Modalità di identificazione e registrazione degli accessi ai dati particolari dopo l'orario di chiusura.

VEDI SCHEMA ALLEGATO

2) Criteri tecnici ed organizzativi per la protezione delle aree e dei locali e procedure di controllo per l'accesso

In questa sezione sono evidenziate una o più delle seguenti misure per la **protezione fisica**:

- Localizzazione e limitazioni all'accesso del data center (localizzazione dei server);
- Locale archivio sito al 1° piano dotato di serratura.

- Dispositivi antintrusione

Allarme collegato alle Forze dell'Ordine per l'intero edificio scolastico

Porta con chiave consegnata solo agli addetti al lavoro per gli Uffici di Segreteria e Presidenza.

Password di accesso al sistema operativo

Password Screen Saver per allontanarsi dalla postazione con sessione di lavoro attiva

- **Dispositivi antincendio** (estintori, manichette, impianti di rilevazione e/o spegnimento automatico);

ESTINTORI NEI LOCALI DI SEGRETERIA

- Sistemi di registrazione degli ingressi e di chiusura dei locali;
Nessuno

- Presenza di un custode e/o di un servizio di vigilanza esterna;
No

- **Custodia in armadi o classificatori ad accesso autorizzato;**

Dati riservati. Armadio con chiave

- **Modalità di custodia delle chiavi;**

Personale ATA

3) Criteri e procedure per assicurare l'integrità e la disponibilità dei dati

In questa sezione sono evidenziate una o più delle seguenti misure per assicurare **l'integrità e la disponibilità dei dati**:

- **Criteri di definizione del salvataggio dei dati**

SERVER

Backup programmato automaticamente una volta alla settimana su hard-disk esterno, il quale viene custodito nell'armadio-server chiuso a chiave nel locale Archivio del 1° piano.

- **Procedure per la conservazione dei backup**

Armadio-server chiuso a chiave nel locale Archivio del 1° piano.

- **Procedure per la verifica della registrazione dei backup;**

Verifica dati automatica pianificata alla fine di ogni backup

- Presenza di un responsabile per l'esecuzione e la verifica dei backup;

- Procedura di sostituzione ed eliminazione dei dispositivi di conservazione obsoleti (cassette, nastri magnetici, supporti ottici).

Eventuali altre misure

- Alimentazione: presenza di gruppi di continuità, sistemi collegati e tempi di funzionamento garantiti;

Gruppo di continuità a protezione del server

- Sistemi dotati di mirroring, in RAID, di tipo hot-swap, dotati di alimentazione ridondante,

sistemi in cluster;

Server dotato di dischi RAID 1 (mirroring). Raid Hardware (controller Raid)

- Procedure di riutilizzo controllato dei supporti di memorizzazione;

Sostituzione (a freddo) di un disco e mirroring automatico gestito dal Bios del controller alla riaccensione del sistema

- Climatizzazione dei locali.

NO locale server

SI locale Segreteria e Presidenza

4) Criteri e procedure per il ripristino dell'accesso ai dati (Piano di disaster recovery)

- Criteri di definizione per il ripristino dei dati (*a seguito di distruzione o danneggiamento dei dati stessi e/o degli strumenti elettronici*);

Restore di windows 2003

- Identificazione degli incidenti "eccezionali" dei sistemi informatici;

Intervento ditta esterna

- Definizione di procedure che assicurino tempi certi di ripristino dei sistemi;

Concordato con ditta esterna

- Verifica periodica delle procedure attivate;

Effettuato Restore di prova

5) Criteri per garantire la predisposizione delle misure minime nel caso di trattamenti affidati all'esterno della struttura aziendale

- Definizione di una corretta applicazione delle misure minime di sicurezza da parte di fornitori esterni relativi alla gestione di dati sensibili o giudiziari.
- Politica di responsabilizzazione dei soggetti esterni (predisposizione di adeguati modelli contrattuali e/o clausole contrattuali).

C - FORMAZIONE E ADEGUAMENTO DEL DOCUMENTO

1) Piani di formazione per gli incaricati del trattamento

Si riportano in questa sezione, gestendola eventualmente con ALLEGATI, il piano formativo in

termini di:

- Calendario e contenuti degli incontri svolti o previsti
- Conservazione della documentazione consegnata
- Registrazione dei partecipanti agli incontri formativi

2) Programma di revisione ed adeguamento

Periodicità dei controlli sull'efficienza ed efficacia delle misure previste nel presente documento *(almeno una volta all'anno e comunque non oltre il 31 marzo di ciascun anno)*.

Modalità di effettuazione del controllo: soggetti obbligati, determinando le misure di cui ogni soggetto è tenuto a verificare l'efficacia e a provvedere ai necessari interventi di adeguamento (Incarichi allegati)

DATA PREVISTA PER ADEGUAMENTO DEL PRESENTE DOCUMENTO:

31 MARZO 2011

DATE PREVISTE PER CORSO DI FORMAZIONE DEL PERSONALE:

Corsi per il personale di segreteria, personale docente e personale ATA : inizio anno scolastico