ISTITUTO COMPRENSIVO STATALE "Via de Andreis "
Via Luigi De Andreis 10 – 20137 Milano
Tel 0288447156 (centralino) fax 02 88447157

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

PRIVACY

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

Milano, 24/03/2015

Prot.nr. 2338/C14

Il titolare del trattamento dei dati
(Dott.ssa Laura Metelli)

Laura Metelli
(firma)

PREMESSA

Questo documento stabilisce le misure di sicurezza organizzative, fisiche e logiche da adottare affinché siano rispettati gli obblighi, in materia di sicurezza del trattamento dei dati effettuato da <<Nome della vostra scuola>>, previsti dal D.L.vo n. 196 del 30/06/2003 "Codice in materia di protezione dei dati personali" e dal Decreto n.305 del 7/12/2006.
Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

1. DEFINIZIONI E RESPONSABILITÀ

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.
CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.
DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.
DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.
DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.
DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.
DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.
INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.
INTERESSATO: il soggetto al quale si riferiscono i dati personali.
RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.
RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.
TITOLARE: il titolare del trattamento è l'Ente (ISTITUTO SCOLASTICO) e la titolarità è esercitata dal rappresentante legale (DIRIGENTE SCOLASTICO), tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.
TRATTAMENTO: qualunque operazione o complesso di operazioni, effettuati anche senza l'ausilio di strumenti elettronici, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, 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, anche se non registrati in una banca di dati.

2. TITOLARE, RESPONSABILI, INCARICATI

Titolare del trattamento dei dati: Dott.ssa Laura Metelli
Responsabile del trattamento dei dati: Dott.ssa Laura Metelli
Responsabile della sicurezza informatica: Prof. Veroni Daniele
Amministratore di sistema: Microtech S.r.l. (Ditta Esterna)
Custode delle password: DSGA Giuseppe Pettinato
Incaricati del trattamento dei dati: come da allegato 1
Incaricati dell'assistenza e della manutenzione degli strumenti elettronici: AXIOS Italia s.r.l.

3. ANALISI DEI RISCHI E INDIVIDUAZIONE DELLE RISORSE DA PROTEGGERE

L'analisi dei rischi consente di:
- acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo;
- 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, ossia la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI
  - DATI PERSONALI SEMPLICI, cioè la classe di dati a rischio intermedio
  - DATI PERSONALI SENSIBILI/GIUDIZIARI, cioè la classe di dati ad alto rischio
  - DATI PERSONALI SANITARI, cioè la classe di dati a rischio altissimo.

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.

4. REGOLAMENTO PER L'IDENTIFICAZIONE DEI DATI (DECRETO 7/12/2006 N.305)

Questo Istituto adotta il regolamento fissato dal DM n.305 del 7/12/2006. In particolare:
- I dati sensibili e giudiziari sono trattati previa verifica della loro pertinenza, completezza e indispensabilità rispetto alle finalità perseguite nei singoli casi, specie quando la raccolta non avvenga presso l'interessato.
- Le operazioni di interconnessione e raffronto con banche di dati di altri titolari del trattamento e di comunicazione a terzi individuate nel presente regolamento sono ammesse soltanto se indispensabili allo svolgimento degli obblighi o compiti di volta in volta indicati e solo per il perseguimento delle rilevanti finalità di interesse pubblico specificate, le operazioni sopraindicate sono inoltre svolte nel rispetto delle disposizioni in materia di protezione dei dati personali e degli altri limiti stabiliti dalla legge e dai regolamenti.
- I raffronti e le interconnessioni con altre informazioni sensibili e giudiziarie sono consentite soltanto previa verifica della loro stretta indispensabilità rispetto ai singoli casi e previa indicazione scritta dei motivi che ne giustificano l'effettuazione. Le operazioni effettuate utilizzando banche di dati di diversi titolari del trattamento e la diffusione di dati sensibili e giudiziari sono ammesse esclusivamente previa verifica della loro stretta indispensabilità in relazione ai singoli casi e nel rispetto dei limiti e con le modalità stabiliti dalle disposizioni legislative che le prevedono.
- Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali.

Le seguenti 7 schede identificano i tipi di dati sensibili o giudiziari e le operazioni su questi eseguibili.

SCHEDA N.1: SELEZIONE E RECLUTAMENTO, A TEMPO INDETERMINATO E DETERMINATO, E GESTIONE DEL RAPPORTO DI LAVORO

Indicazione del trattamento e descrizione riassuntiva del contesto

Selezione e reclutamento, a tempo indeterminato e determinato, e gestione del rapporto di lavoro del personale dipendente dell'Amministrazione centrale e periferica del Ministero dell'istruzione, dirigente, docente, educativo ed ATA delle istituzioni scolastiche ed educative, personale IRRE, dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato.

Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione alla gestione

e alla cessazione del rapporto di lavoro.

1. I dati inerenti lo stato di salute sono trattati per: l'adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzioni del personale appartenente alle c.d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative, pensionistiche e previdenziali obbligatori e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi per il personale e provvidenze, collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;

2. I dati idonei a rilevare l'adesione a sindacati o ad organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o all'esercizio dei diritti sindacali;

3. I dati sulle convinzioni religiose per la concessione di permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche ai fini del reclutamento dei docenti di religione;

4. I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;

5. I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato;

6. Le informazioni sulla vita sessuale possono desumersi solo in caso di eventuale rettificazione di attribuzione di sesso.

I dati sono raccolti su iniziativa degli interessati o previa richiesta dell'Ufficio presso i medesimi interessati, ovvero presso altri soggetti pubblici o privati, e sono trattati, sia in forma cartacea che telematica, per l'applicazione dei vari istituti disciplinati dalla legge e dai regolamenti in materia di selezione, reclutamento, gestione giuridica, economica, previdenziale, pensionistica, aggiornamento e formazione del personale.

Finalità di rilevante interesse pubblico perseguito

- ART. 112: "instaurazione e gestione da parte dei soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato"
- ART. 62: "rilascio di documenti di riconoscimento"
- ART. 67: "attività di controllo e ispettive"
- ART. 68: "applicazione della disciplina in materia di concessione, liquidazione, modifica e revoca di benefici economici, agevolazioni, elargizioni, altri emolumenti e abilitazioni"
- ART. 70: "applicazione della legge 8/7/1998 n. 230 e delle altre disposizioni di legge in materia obiezione di coscienza"
- ART. 72: "rapporti con Enti di culto"
- ART. 73: "supporto al collocamento e avviamento al lavoro"

Tipi di dati trattati

- CONVINZIONI religiose, filosofiche, d'altro genere
- CONVINZIONI sindacali
- STATO DI SALUTE: patologie attuali e pregresse, terapie in corso, dati sulla salute relativi anche ai familiari
- VITA SESSUALE (solo in caso di rettificazione di attribuzione di sesso)
- DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e), del Codice)

Operazioni eseguite: particolari forme di trattamento

Interconnessioni e raffronti di dati con altro titolare: Amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive rese ai fini del DPR 445/2000.

Comunicazione ai seguenti soggetti per le seguenti finalità: Servizi sanitari competenti per le visite fiscali e per l'accertamento dell'idoneità all'impiego; Organi preposti al riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001; Organi preposti alla vigilanza in materia di igiene e sicurezza sui luoghi di lavoro (d.lg. n. 626/1994); Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza a fini assistenziali e previdenziali, nonché per la denuncia delle malattie professionali o infortuni sul lavoro ai sensi del d.P.R. n. 1124/1965; Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della L. 68/1999; Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali; Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità; Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione Cattolica ai sensi della Legge. 18/7/2003, n.186; Organi di controllo (Corte dei Conti e MEF) al fine del controllo di legittimità e annotazione della spesa

dei provvedimenti di stato giuridico ed economico del personale ex Legge n. 20/94 e D.P.R. 20 febbraio 1998, n.38; Agenzia delle Entrate ai fini degli obblighi fiscali del personale ex Legge 30/12/1991, n. 413; MEF e INPDAP per la corresponsione degli emolumenti connessi alla cessazione dal servizio ex Legge 8 agosto 1995, n. 335; Presidenza del Consiglio dei Ministri per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive (art.50, comma 3, d.lg. n.165/2001).

Operazioni eseguite: altre tipologie più ricorrenti di trattamenti

- RACCOLTA: presso gli interessati e presso terzi
- ELABORAZIONE: in forma cartacea e con modalità informatizzate

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N.2: GESTIONE DEL CONTENZIOSO E PROCEDIMENTI DISCIPLINARI

Indicazione del trattamento e descrizione riassuntiva del contesto

Il trattamento dei dati sensibili e giudiziari concerne tutte le attività relative alla difesa in giudizio del Ministero dell'istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

Finalità di rilevante interesse pubblico perseguito

- ART. 112: "instaurazione e gestione da parte dei soggetti pubblici di rapporti di lavoro di qualunque tipo, dipendente o autonomo, anche non retribuito o onorario o a tempo parziale o temporaneo, e di altre forme di impiego che non comportano la costituzione di un rapporto di lavoro subordinato"
- ART. 67: "attività di controllo e ispettive"
- ART. 71: "attività sanzionatorie e di tutela".

Tipi di dati trattati

- ORIGINE razziale ed etnica
- CONVINZIONI religiose, filosofiche, d'altro genere
- CONVINZIONI politiche e sindacali
- STATO DI SALUTE: patologie attuali e pregresse, terapie in corso, dati sulla salute relativi anche ai familiari
- VITA SESSUALE
- DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e), del Codice)

Operazioni eseguite: particolari forme di trattamento

Comunicazione con altri soggetti pubblici o privati: Ministero del Lavoro e delle Politiche Sociali per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi a Collegi di conciliazione ex D.Lgs. 30 marzo 2001, n. 165; Organi arbitrali per lo svolgimento delle procedure arbitrali ai sensi dei CCNL di settore; Avvocature dello Stato per la difesa erariale e consulenza presso gli organi di giustizia; Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria per l'esercizio dell'azione di giustizia; Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

Operazioni eseguite: altre tipologie più ricorrenti di trattamenti

- RACCOLTA: presso gli interessati e presso terzi
- ELABORAZIONE: in forma cartacea e con modalità informatizzate

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N.3: ORGANISMI COLLEGIALI E COMMISSIONI ISTITUZIONALI

Indicazione del trattamento e descrizione riassuntiva del contesto

Il trattamento dei dati sensibili è necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali.

Il dato sensibile trattato è quello dell'appartenenza alle organizzazioni sindacali, con riferimento agli organismi o comitati che richiedano la partecipazione di rappresentati delle organizzazioni sindacali.

Finalità di rilevante interesse pubblico perseguito

- ART. 65: "pubblicità dell'attività di organi"
- ART. 95: "dati sensibili e giudiziari relativi alle finalità di istruzione e di formazione in ambito scolastico, professionale, superiore o universitario".

Tipi di dati trattati

- CONVINZIONI sindacali

- DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e), del Codice)

Operazioni eseguite: altre tipologie più ricorrenti di trattamenti

- RACCOLTA: presso gli interessati e presso terzi
- ELABORAZIONE: in forma cartacea e con modalità informatizzate

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N.4: ATTIVITÀ PROPEDEUTICHE ALL'AVVIO DELL'ANNO SCOLASTICO

Indicazione del trattamento e descrizione riassuntiva del contesto

I dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali. Nell'espletamento delle attività propedeutiche all'avvio dell'anno scolastico da parte delle istituzioni scolastiche, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana;
- alle convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- allo stato di salute, per assicurare l'erogazione del sostegno agli alunni disabili e per la composizione delle classi;
- alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione; i dati giudiziari emergono anche nel caso in cui l'autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell'alunno nonché nei confronti degli alunni che abbiano commesso reati.

Finalità di rilevante interesse pubblico perseguito

Le finalità di cui agli artt. 68, 73, 86, 95 del D.Lgs. 30 giugno 2003, n. 196.

Tipi di dati trattati

- ORIGINE razziale ed etnica
- CONVINZIONI religiose e d'altro genere
- STATO DI SALUTE: patologie attuali e pregresse, terapie in corso, dati sulla salute relativi anche ai familiari
- DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e), del Codice)

Operazioni eseguite: particolari forme di trattamento

Comunicazione ai seguenti soggetti per le seguenti finalità: agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgsl. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio; ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio; c) alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro Handicap di istituto e per la predisposizione e verifica del Piano Educativo Individualizzato, ai sensi della Legge 5 febbraio 1992, n. 104.

Operazioni eseguite: altre tipologie più ricorrenti di trattamenti

- RACCOLTA: presso gli interessati e presso terzi
- ELABORAZIONE: in forma cartacea e con modalità informatizzate

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N.5: ATTIVITÀ EDUCATIVA, DIDATTICA E FORMATIVA, DI VALUTAZIONE

Indicazione del trattamento e descrizione riassuntiva del contesto

Nell'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, da parte delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti ed educandati e scuole speciali, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche per favorire l'interazione degli alunni con cittadinanza non italiana;
- alle convinzioni religiose per garantire la libertà di credo religioso;
- allo stato di salute, per assicurare l'erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell'insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;
- ai dati giudiziari, per assicurare il diritto allo studio anche a soggetti sottopostl a regime di detenzione;
- alle convinzioni politiche, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori.

I dati sensibili possono essere trattati per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze.

Finalità di rilevante interesse pubblico perseguito

Le finalità di cui agli artt. 68, 73, 86, 95 del D.Lgs. 30 giugno 2003, n. 196.

Tipi di dati trattati

- ORIGINE razziale ed etnica
- CONVINZIONI religiose, filosofiche e d'altro genere
- CONVINZIONI politiche
- STATO DI SALUTE: patologie attuali e pregresse, terapie in corso, dati sulla salute relativi anche ai familiari
- VITA SESSUALE
- DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e), del Codice)

Operazioni eseguite: particolari forme di trattamento

Comunicazione ai seguenti soggetti per le seguenti finalità: alle altre istituzioni scolastiche, statali e non statali, per la trasmissione della documentazione attinente la carriera scolastica degli alunni, limitatamente ai dati indispensabili all'erogazione del servizio; agli Enti Locali per la fornitura dei servizi ai sensi del D. Lgs. 31 marzo 1998, n. 112, limitatamente ai dati indispensabili all'erogazione del servizio; ai gestori pubblici e privati dei servizi di assistenza agli alunni e di supporto all'attività scolastica, ai sensi delle leggi regionali sul diritto allo studio, limitatamente ai dati indispensabili all'erogazione del servizio; agli Istituti di assicurazione per denuncia di infortuni e per la connessa responsabilità civile; all'INAIL per la denuncia di infortuni ex-DPR 30/6/1965, n. 1124; alle AUSL e agli Enti Locali per il funzionamento dei Gruppi di Lavoro di istituto per l'Handicap e per la predisposizione e la verifica del Piano Educativo Individuale, ai sensi della Legge 5 febbraio 1992, n. 104; ad aziende, imprese e altri soggetti pubblici o privati per tirocini formativi, stages e alternanza scuola-lavoro, ai sensi della Legge 24 giugno 1997, n. 196 e del D.Lgs. 21 aprile 2005, n. 77 e, facoltativamente, per attività di rilevante interesse sociale ed economico, limitatamente ai dati indispensabili all'erogazione del servizio.

Operazioni eseguite: altre tipologie più ricorrenti di trattamenti

- RACCOLTA: presso gli interessati e presso terzi
- ELABORAZIONE: in forma cartacea e con modalità informatizzate

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N.6: SCUOLE NON STATALI

Indicazione del trattamento e descrizione riassuntiva del contesto

Nell'ambito delle procedure di accreditamento e autorizzazione delle istituzioni scolastiche non statali, l'Amministrazione scolastica periferica esercita attività di: concessione o revoca delta parità; concessione della parifica (scuola primaria); concessione o revoca del riconoscimento legale (scuote secondarie); concessione o revoca della presa d'atto.

Dati sensibili emergono nel caso di attività di vigilanza e controllo effettuate dall'Amministrazione centrale e periferica che prevedono l'accesso ai fascicoli personali dei docenti e degli alunni. Dati sensibili sono, inoltre, trattati dai dirigenti scolastici delle scuole dell'infanzia e primarie incaricati della vigilanza sulle scuole non statali provviste di autorizzazione.

Finalità di rilevante interesse pubblico perseguito

Le finalità di cui all'art. 67 del D.Lgs. 30 giugno 2003, n. 196.

Tipi di dati trattati

- ORIGINE razziale ed etnica
- CONVINZIONI religiose, filosofiche e d'altro genere
- CONVINZIONI politiche
- STATO DI SALUTE: patologie attuali e pregresse, terapie in corso, dati sulla salute relativi anche ai familiari
- DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e), del Codice)

Operazioni eseguite: altre tipologie più ricorrenti di trattamenti

- RACCOLTA: presso gli interessati e presso terzi
- ELABORAZIONE: in forma cartacea e con modalità informatizzate

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

SCHEDA N.7: RAPPORTI SCUOLA-FAMIGLIE: GESTIONE DEL CONTENZIOSO

Indicazione del trattamento e descrizione riassuntiva del contesto

Il trattamento di dati sensibili e giudiziari concerne tutte le attività connesse alla instaurazione di contenziosi (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce all' autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.

Finalità di rilevante interesse pubblico perseguito

Le finalità di cui agli artt. 67 e 71 del D.Lgs. 30 giugno 2003, n. 196.

Tipi di dati trattati

- ORIGINE razziale ed etnica
- CONVINZIONI religiose, filosofiche e d'altro genere
- CONVINZIONI politiche e sindacali
- STATO DI SALUTE: patologie attuali e pregresse, terapie in corso, dati sulla salute relativi anche ai familiari
- VITA SESSUALE
- DATI DI CARATTERE GIUDIZIARIO (art 4, comma 1, lett. e), del Codice)

Operazioni eseguite: particolari forme di trattamento

Comunicazione con altri soggetti pubblici e privati: Avvocature dello Stato, per la difesa erariale e consulenza presso gli organi di giustizia; Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia; Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza.

Operazioni eseguite: altre tipologie più ricorrenti di trattamenti

- RACCOLTA: presso gli interessati e presso terzi
- ELABORAZIONE: in forma cartacea e con modalità informatizzate

Altre operazioni ordinarie: registrazione, organizzazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, blocco, cancellazione e distruzione.

Per ulteriori dettagli vedere gli Allegati 1 e 3.

5. INDIVIDUAZIONE DELLE MINACCE E DELLE VULNERABILITÀ

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse indicate nel precedente punto 3.

RISCHIO	Deliberato	Accidentale	Ambientale
Terremoto			x
Inondazione	x	x	x
Uragano			x
Fulmine			x
Bombardamento	x	x	
Fuoco	x	x	
Uso di armi	x	x	
Danno volontario	x		
Interruzione di corrente	x	x	
Interruzione di acqua	x	x	
Interruzione di aria condizionata	x	x	
Guasto hardware		x	
Linea elettrica instabile		x	x
Temperatura e umidità eccessive			x
Polvere			x
Radiazioni elettromagnetiche		x	
Scariche elettrostatiche		x	
Furto	x		
Uso non autorizzato dei supporti di memoria	x		
Deterioramento dei supporti di memoria		x	
Errore del personale operativo		x	
Errore di manutenzione		x	
Masquerading dell'identificativo dell'utente	x		
Uso illegale di software	x	x	
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	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

Negli elenchi seguenti sono descritte le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nella tabella precedente.

Infrastruttura: mancanza di protezione fisica dell'edificio (porte, finestre, inferriate, ecc.); mancanza di controllo di accesso; linea elettrica instabile; edificio suscettibile ad allagamenti.

Hardware: mancanza di sistemi di ridondanza; suscettibilità a variazioni di tensione; suscettibilità a variazioni di temperatura; suscettibilità a umidità, polvere, sporcizia; suscettibilità a radiazioni elettromagnetiche; manutenzione insufficiente; carenze di controllo di configurazione.

Comunicazioni: linee di comunicazione o giunzioni non protette; mancanza di autenticazione; trasmissione password in chiaro; mancanza di prova di ricezione/invio; presenza di linee dial-up (con modem) o connessioni a linea pubblica non protette; traffico sensibile non protetto; gestione inadeguata della rete.

Documenti cartacei: locali non protetti; carenza di precauzioni nell'eliminazione; non controllo delle copie.

Software: interfaccia uomo-macchina complicata; mancanza di identificazione/autenticazione; mancanza del registro delle attività (log); errori noti del software; tabelle di password non protette; carenza/assenza di gestione delle password; scorretta politica dei diritti di accesso; carenza di controllo nel caricamento e uso di software; 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.

Personale: carenza di personale; mancanza di supervisione degli esterni; formazione insufficiente sulla sicurezza; carenza di consapevolezza; uso scorretto di hardware/software; carenza di monitoraggio; carenza nelle politiche per i mezzi di comunicazione; procedure di reclutamento inadeguate.

6. 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, 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 di questo Istituto Scolastico;
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti;
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'Istituto Scolastico;

- i locali ad accesso controllato sono provvisti di sistema di allarme e di estintore;
- Si (armadi blindati, apparecchiature di continuità, sistemi di condizionamento, sistemi antincendio). Si prevede nel corso dell'anno, disponibilità finanziaria permettendo, l'acquisto di armadi ignifughi)

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 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;
- il protocollo riservato è accessibile solo al Titolare del trattamento ed è conservato Cassaforte Presidenza

Per il trattamento dei soli dati cartacei sono adottate le seguenti disposizioni:
- si accede ai soli dati strettamente necessari allo svolgimento delle proprie mansioni e si utilizzano archivi con accesso selezionato;
- atti e documenti devono essere restituiti al termine delle operazioni;
- è vietato fotocopiare, fotografare, acquisire tramite scanner documenti senza l'autorizzazione del responsabile del trattamento;
- è vietato esportare documenti o copie dei documenti all'esterno dell'Istituto senza l'autorizzazione del responsabile del trattamento;
- 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.

7. NORME PER IL PERSONALE, INCIDENT RESPONSE E PIANO DI FORMAZIONE

Tutti i dipendenti concorrono alla realizzazione della sicurezza; pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa e indicate nel punto 3, nel rispetto di quanto stabilito in questo documento e dal regolamento di utilizzo della rete (Allegato 4).
Per l'Incidente Response e Ripristino, vedere l'Allegato 3.
La formazione degli incaricati viene effettuata all'ingresso in servizio, in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti rilevanti rispetto al 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.
Si

Il piano prevede inoltre la pubblicazione di normativa ed ordini di servizio in bacheca situata Bacheca ingresso sede centrale e sito web della scuola

8. 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 n.196 del 30/06/2003. 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.

9. 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
- Lettera di incarico per il responsabile del trattamento
- Lettera di incarico per il responsabile della sicurezza informatica
- Lettera di incarico per l'amministratore di sistema
- Lettera di incarico per il custode delle password
- Lettere di incarico per il trattamento dei dati

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

Milano, 24/03/2015

Il titolare del trattamento dei dati
(Dott.ssa Laura Metelli)

Laura Metelli
(firma)

ISTITUTO COMPRENSIVO STATALE "Via de Andreis "
Via Luigi De Andreis 10 – 20137 Milano
Tel 0288447156 (centralino) fax 02 88447157

DPS - ALLEGATO 1: ELENCO TRATTAMENTI DEI DATI

Tabella 1 - Elenco dei trattamenti dei dati

La seguente tabella riporta il trattamento dei dati personali attraverso l'indicazione della finalità perseguita o dell'attività svolta e delle categorie di persone cui i dati si riferiscono.
Natura dei dati trattati: indica 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.
La struttura di riferimento indica la struttura all'interno della quale viene effettuato il trattamento. Se un trattamento comporta l'attività di diverse strutture, sono indicate, oltre quella che cura primariamente l'attività, le altre strutture che concorrono al trattamento.
Per "strumenti utilizzati" si intendono strumenti elettronici e altre tipologie di contenitori.

Finalità perseguita o attività svolta	Categorie di interessati	Natura dei dati trattati	Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati
Trattamento dati dipendenti per attività amministrative	dipendenti (dirigente, docenti, ATA)	personali semplici e sensibili	Segreteria Amministrativa	Presidenza, Sala Server Uffici, Ufficio DSGA, Protocollo	Trattamenti su supporto cartaceo (registri dei docenti, registri di classe, registro voti, libri dei verbali di CdC, elaborati) e su sopporto elettronico (Axios, documenti Office, Outlook per Posta Elettronica)
Trattamento dati alunni e loro famiglie per attività amministrative	alunni e loro famiglie	personali semplici e sensibili	Segreteria Didattica e amministrazione	Protocollo, Presidenza	Trattamenti su supporto cartaceo (fascicoli alunni, registri matricola, certitificati medici, registro infortuni e relative pratiche) e su sopporto elettronico (Axios e documenti Office)
Trattamento dati docenti per la didattica e le altre attività correlate	docenti	personali semplici	Segreteria Didattica e amministrazione	Presidenza, Server web, Archivio e Sala insegnanti	Trattamenti su supporto cartaceo (registri dei docenti, registri di classe, registro voti, libri dei verbali di CdC, elaborati) e su sopporto elettronico (Axios, documenti Office, Outllok per Posta Elettronica)

Tabella 2 - Descrizione della struttura organizzativa e dei trattamenti

Struttura: sono le indicazioni delle strutture dell'Istituto menzionate nella Tabella 1.
Trattamenti effettuati nella struttura: indica i trattamenti di competenza di ciascuna struttura.
Compiti e responsabilità della struttura: descrive sinteticamente i compiti e le responsabilità della struttura rispetto ai trattamenti di competenza.

Struttura	Trattamenti effettuati nella struttura	Compiti e responsabilità della struttura
Segereteria - Ufficio DSGA	Trattamenti per lo svolgimento dei compiti di gestione amministrativa (tenuta dei dati connessi all'espletamento di procedimenti amministrativi, attività contrattuale, gestione di beni, procedure di bilancio)	Acquisizione e caricamento dei dati, consultazione, stampa, comunicazione a terzi, gestione tecnica operativa della base dati, salvataggi/ripristini di documenti Office e software di utilizzo in locale
Presidenza	Trattamenti per lo svolgimento dei compiti istituzionali (gestione della corrispondenza; tenuta del protocollo riservato, dei verbali del consiglio d'Istituto; Elenchi Studenti, Docenti, Ata) ed attività connesse ai rapporti con organi pubblici	come sopra
Segereteria - Didattica e Amministrativa	Trattamenti strumentali all'offerta formativa (registrazione di iscrizioni, assenze, valutazioni, partecipazione a attività del POF; condizioni sanitarie/economiche di studenti e famigliari, documentazione per insegnamenti facoltativi)	come sopra
Segereteria - Amministrativa	Trattamenti per la gestione contabile dell'Istituto (liquidazioni di parcelle, mandati, registri e inventari , dati fornitori)	come sopra

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

La seguente tabella riporta le indicazioni per ogni incaricato del trattamento, con le mansioni che il dipendente deve svolgere e con le operazioni di trattamento dei dati cui può accedere l'incaricato. Struttura di riferimento è la struttura di appartenenza dell'incaricato.
Negli Strumenti utilizzati è indicato, ad esempio, il numero di inventario o un codice identificativo del PC. Nelle Responsabilità aggiuntive si indicano le eventuali ulteriori responsabilità rispetto all'incarico per il trattamento dei dati.
Natura dei dati trattati: indica la classe di rischio dei dati trattati tenendo presente la seguente classificazione

Nome Cognome	Mansioni	Operazioni	Struttura di riferimento	Strumenti utilizzati	Responsabilità aggiuntive
Dott.ssa Laura Metelli	Dirigente scolastico	responsabilità gestione Istituto	Presidenza	PC	titolare del trattamento
Giuseppe Pettinato	DSGA	responsabile attività amministrativa	Segreteria	PC	responsabile del trattamento, amministratore di sistema
Mignani Catia	Ass. Amm.	segreteria amministrativa	Segreteria	PC	Gestione personale Docente ed ATA
Puerari Cinzia	Ass. Amm.	segreteria amministrativa	Segreteria	PC	Gestione personale Docente ed ATA
Brucculeri Graziella	Ass. Amm.	segreteria amministrativa	Segreteria	PC	Gestione personale Docente ed ATA
Caserio Paola Lucilla	Ass. Amm.	segreteria amministrativa	Segreteria	PC	Gestione Protocollo
Lanzi Roberta	Ass. Amm.	segreteria amministrativa	Segreteria	PC	Gestione Affari Generali
Borri Maria Cristina	Ass. Amm.	segreteria Didattica	Segreteria	PC	Gestione alunni
Melidoni Rita	Ass. Amm.	Segreteria didattica	Segreteria	PC	Gestione alunni
Leuzzi Anna	Ass. Amm.	Segreteria Amministrativa	Segreteria	PC	Gest. Affari Generali e supporto Contabilità

DPS - ALLEGATO 2: MINACCE

ISTITUTO COMPRENSIVO STATALE "VIA DE ANDREIS"

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 sia dall'interno sia dall'esterno dell'Istituto e sono relative:

- all'utilizzo della LAN/Intranet (interne, esterne wireless);
- all'utilizzo di 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. Lo spoofing si manifesta come attività di falsificazione di alcuni dati telematici, come l'indirizzo IP o il mittente dei messaggi di posta elettronica.

PACKET SNIFFING: Acquisizione di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. 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, il computer sia stato oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

PORT SCANNING: Serie programmata di tentativi di accesso con lo scopo di rilevare le caratteristiche tecniche del computer "attaccato" e le eventuali vulnerabilità.

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 può provocare la saturazione della casella e la conseguente impossibilità a ricevere ulteriori messaggi.

PASSWORD CRACKING: Sono programmi che servono per decodificare le password.

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

WORM: Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano notevoli 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 funzionamento.

LOGIC BOMB Appartengono alla categoria dei virus e sono programmi che contengono 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.

DOS (DENIAL OF SERVICE) Attacco 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 è riservato esclusivamente all'amministratore di sistema per la misura/diagnostica delle prestazioni della rete dell'Istituto; tali programmi non sono in alcun caso utilizzati su reti esterne a quella dell'Istituto.

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

MINACCE A CUI SONO SOTTOPOSTI I DATI TRATTATI

Le principali minacce ai dati trattati sono:

- accesso non autorizzato (visione, modifica, cancellazione, esportazione) agli archivi contenenti le informazioni riservate 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 e deterioramento nel tempo (invecchiamento dei supporti);
- imperizia degli utilizzatori;
- sabotaggio;
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media.

DPS - ALLEGATO 3: MISURE, INCIDENT RESPONSE, RIPRISTINO

ISTITUTO COMPRENSIVO STATALE "VIA DE ANDREIS"

Tabella 1 - Descrizione Personal Computer

Sono elencati tutti i computer utilizzati, sia connessi sia non connessi alla rete, con indicazione del tipo di computer, del sistema operativo, del software applicativo utilizzato e della connessione alla rete.
I PC descritti in questa tabella non prendono in considerazione quelli presenti nei laboratori didattici.

Identificativo del PC	Tipo PC	Sistema operativo	Software utilizzato	Rete
SERVER- (Protocollo)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC- (DS)	INTEL PENTIUM	Windows 7.1	Office, Internet Explorer e CHROME	Internet e Lan
PC- (DSGA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-Lanzi (AA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-Caserio (AA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-IEUZZI (AA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-Puerari (AA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-Mignani (AA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-Brucculeri (AA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-Borri (AA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-Melidoni (AA)	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan
PC-Vicepreside	INTEL PENTIUM	Windows XP	Office, Internet Explorer e CHROME	Internet e Lan

Tabella 2 - Connettività Internet

La seguente tabella riporta l'elenco delle connettività ad Internet, indicandone il tipo, le apparecchiature di comunicazione e i provider (fornitori di connettività).

Connettività	Apparecchiature di comunicazione	Provider
Fibra Ottica	Router	Fastweb S.p.A.

MISURE DI CARATTERE ELETTRONICO/INFORMATICO

Le misure di carattere elettronico/informatico adottate per segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, per gestire le copie di salvataggio dei dati e degli applicativi, per assicurare l'integrità dei dati, per proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi, sono:

- utilizzo di server con configurazioni di ridondanza (misura già attiva);
- presenza di gruppi di continuità elettrica per i server (misura già attiva);
- attivazione di un sistema di backup centralizzato e automatizzato con periodicità settimanale e storico di un mese (misura già attiva); i responsabili delle copie sono indicati nell'Allegato 1 relativo al censimento dei trattamenti dei dati;
- installazione di un firewall per proteggere la rete dagli accessi indesiderati attraverso internet (misura già attiva);
- definizione delle regole per la gestione delle password di seguito specificate (misura già attiva);
- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows 9x e Windows Me;
- installazione di un sistema antivirus client/server su tutte le postazioni di lavoro, configurato per eseguire la procedura di aggiornamento in automatico con frequenza giornaliera e la scansione periodica dei supporti di memoria (la misura sarà completamente attiva entro 04/2015);
- 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 logica della rete locale delle segreterie da quella dei laboratori didattici (misura già attiva);

REGOLE PER LA GESTIONE DELLE PASSWORD

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato user-id) e password personale.
User-id e password iniziali sono assegnati dal custode delle password.
User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.
La password deve essere composta da almeno 8 caratteri alfanumerici.
La password non deve contenere elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore; deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.
Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.

Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema; esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.
In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione, l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che devono essere custodite in cassaforte.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:
- le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
- per la definizione/gestione della password devono essere rispettate le seguenti regole:
1. la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
2. la password non deve essere uguale allo user-id;
3. al primo accesso la password ottenuta dal custode delle password deve essere cambiata;
4. la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
5. la password è segreta: non deve essere comunicata ad altri e va custodita con diligenza e riservatezza;
6. 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 sono realizzate su NAS: hard disk di rete e sono conservate in armadio BLINDATO;
- 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 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 (Ufficio Amministrativo) e l'utilizzo è consentito unicamente agli incaricati del trattamento Assistenti Amministrativi.
La manutenzione degli elaboratori, che può prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS
Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:
- non lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;
- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, penne usb, ...) 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;
- 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 poiché molti 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 non autorizzate dall'amministratore di sistema;
- attivare gli aggiornamenti automatici del sistema operativo oppure consultare con periodicità almeno mensile la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- attivare le condivisioni dell'HD in scrittura solo se autorizzati dall'amministratore di sistema;
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);
- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc.) fornite dal costruttore.

Nel caso di sistemi danneggiati seriamente da virus, l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati, seguendo la procedura indicata:
- formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo;
- installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
- reinstallare i programmi applicativi a partire dai supporti originali;
- effettuare il RESTORE dei soli dati a partire da una copia di backup recente; i programmi eseguibili non devono essere ripristinati dalla copia di backup poiché potrebbe essere infetti;
- effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
- ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

INCIDENT RESPONSE E RIPRISTINO

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino anomalie, quali discrepanze nell'uso degli user-id, modifica e sparizione di dati, cattive prestazioni del sistema.
In caso di incidente, sono considerate le seguenti priorità:
1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone, si procedere a:
1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3.spegnere correttamente il sistema oggetto dell'incidente; una volta spento, il sistema 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, cioè quando non vi è frode, danno, abuso e non è configurabile alcun 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 segue:
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 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.

DPS - ALLEGATO 4: REGOLAMENTO PER L'UTILIZZO DELLA RETE

ISTITUTO COMPRENSIVO STATALE "VIA DE ANDREIS"

1 - OGGETTO E AMBITO DI APPLICAZIONE

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

2 - PRINCIPI GENERALI - DIRITTI E RESPONSABILITÀ

Questo Istituto Scolastico 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.

3 - ABUSI E ATTIVITÀ VIETATE

E' vietato ogni tipo di abuso, cioè 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.
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 dell'Istituto;
- violare la riservatezza di altri utenti o di terzi;
- agire deliberatamente con attività che influenzino negativamente la regolare operatività della rete e ne restringano l'utilizzabilità e le prestazioni per altri utenti;
- agire deliberatamente con attività che distraggano risorse (persone, capacità, elaboratori);
- fare o permettere ad altri trasferimenti non autorizzati di informazioni (software, basi dati, ecc.);
- installare o eseguire deliberatamente o diffondere su qualunque computer e sulla rete, programmi destinati a danneggiare o sovraccaricare i sistemi o la rete (es. 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 dell'Istituto per scopi personali e/o non istituzionali;
- utilizzare la posta elettronica con le credenziali di accesso di altri utenti;
- utilizzare la posta elettronica inviando e ricevendo materiale che violi le leggi.
- utilizzare l'accesso ad Internet per scopi personali;
- accedere direttamente ad Internet con modem collegato al proprio Personal Computer se non espressamente autorizzati e per particolari motivi tecnici;
- connettersi ad altre reti senza autorizzazione;
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare le attività degli utenti, leggere copiare o cancellare file e software di altri utenti, senza averne l'autorizzazione esplicita;
- usare l'anonimato o servirsi di risorse che consentano di restare anonimi sulla rete;

- inserire o cambiare la password del bios, se non dopo averla espressamente comunicata all'amministratore di sistema e essere stati espressamente autorizzati;
- abbandonare il posto di lavoro lasciandolo incustodito o accessibile, come specificato nell'allegato 3.

4 - ATTIVITÀ CONSENTITE

E' consentito all'amministratore di sistema:
- monitorare o utilizzare qualunque tipo di sistema informatico o elettronico per controllare il corretto utilizzo delle risorse di rete, dei client e degli applicativi, per copiare o rimuovere file e software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- creare, modificare, rimuovere o utilizzare qualunque password, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori. L'amministratore darà comunicazione dell'avvenuta modifica all'utente che provvederà ad informare il custode delle password come da procedura descritta nell'allegato 3;
- rimuovere programmi software, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori;
- rimuovere componenti hardware, solo se rientrante nelle normali attività di manutenzione, gestione della sicurezza e della protezione dei dati e nel pieno rispetto di quanto previsto riguardo ai diritti dei lavoratori.

5 - SOGGETTI CHE POSSONO AVERE ACCESSO ALLA RETE

Hanno diritto ad accedere alla rete dell'Istituto Scolastico 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.
Le informazioni e le attività eseguite sulla rete informatica e telematica dell'Istituto 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.

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.

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 dell'Istituto.