

Il Dirigente dell'Istituzione Scolastica, Prof. Maurizio De Renzi

- VISTO il decreto legislativo 30 giugno 2003, n. 196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 34 ss., nonché l'allegato B del suddetto d.lgs., contenente il Disciplinare tecnico in materia di misure minime di sicurezza.
- CONSIDERATO che l'Istituzione Scolastica Istituto di Istruzione Superiore Statale L. ANNEO SENECA con sede in Via Albergotti 35, 00167 ROMA in quanto dotata di un autonomo potere decisionale, ai sensi dell'art. 28 del d.lgs. n. 196 del 2004, deve ritenersi titolare del trattamento di dati personali;
- ATTESO che la suddetta Istituzione scolastica è tenuta a prevedere ed applicare le misure minime di sicurezza di cui agli artt. 31 e ss. del d.lgs. n. 196 del 2003, adotta il presente

DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

L'Istituzione scolastica, per l'espletamento della funzione didattica e formativa, raccoglie e tratta dati personali dei soggetti coinvolti nell'offerta formativa ovvero dei destinatari della stessa, anche con l'ausilio di soggetti esterni, ai sensi del punto 19 dell'Allegato "B", talché si precisano i seguenti elementi:

1. Elenco dei trattamenti di dati personali;
2. Elenco dei dati personali di natura comune, sensibile o giudiziaria
3. Responsabile trattamento dati
4. Ambito dei trattamenti.
5. Analisi dei rischi incombenti sui dati;
6. Misure adottate per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
7. Criteri e modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
8. Programma degli interventi formativi degli incaricati del trattamento;
9. Criteri previsti per garantire il rispetto delle misure minime per i trattamenti di dati personali affidati all'esterno della struttura;
10. Trattamenti di dati personali sensibili o giudiziari con strumenti elettronici affidati all'esterno.

1. ELENCO DEI TRATTAMENTI DI DATI PERSONALI.

Finalità:

Al fine di perseguire le finalità istituzionali, l'Istituzione scolastica tratta dati personali (sia comuni che sensibili o giudiziari) di studenti, personale dipendente, fornitori. I trattamenti sono effettuati, anche mediante strumenti elettronici, per le seguenti finalità:

- adempimento agli obblighi di fonte legislativa, nazionale o comunitaria, regolamentare o derivante da atti amministrativi;
- somministrazione dei servizi formativi;
- gestione e formazione del personale, nelle sue varie componenti (docente e non docente, in ruolo presso altri apparati pubblici);
- adempimenti assicurativi;
- tenuta della contabilità;
- gestione delle attività informative curate ai sensi della legge 7 giugno 2000, n. 150 contenente la "Disciplina delle attività di informazione e di comunicazione delle pubbliche amministrazioni";
- attività strumentali alle precedenti.

Fonte dei dati:

I dati trattati sono conservati su supporti informatici e/o cartacei e sono noti all'istituzione scolastica, in ragione della produzione:

- -di atti e/o dichiarazioni provenienti da soggetti interessati a fruire direttamente, o a beneficio dei minori sottoposti alla potestà ex art. 316 c.c., dei servizi formativi;
- -documenti contabili connessi alla fornitura di prestazioni e/o di servizi e/o di lavori;
- -documentazione bancaria, finanziaria e/o assicurativa;
- -documenti inerenti il rapporto di lavoro, finalizzati anche agli adempimenti retributivi e/o previdenziali.

2. ELENCO DEI DATI PERSONALI DI NATURA COMUNE O SENSIBILE.

Sulla scorta delle precisazioni sopra elencate, l'istituzione scolastica, sulla base di una prima ricognizione, con salvezza della possibilità di procedere a successive integrazioni e/o correzioni entro il 31.3.2006, dichiara, con riferimento ai destinatari o familiari dei destinatari dell'offerta formativa ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo, coinvolti in rapporti negoziali con l'istituzione scolastica, o aspiranti ad assumere tale ruolo, di trattare i dati di seguito elencati:

- 1) Dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del d.lgs. n. 196 del 2003, univocamente riconducibili ad un soggetto fisico, identificato o identificabile, quali nominativo, dati di nascita, residenza, domicilio, stato di famiglia, codice fiscale, stato relativo all'adempimento degli obblighi di leva.
- 2) Dati identificativi, ai sensi dell'art. 4, comma 1, lettere b) e c) del d.lgs. n. 196 del 2003, univocamente riconducibili a persone giuridiche, enti o associazioni, inerenti la forma giuridica, la data di costituzione, la sede, il domicilio, l'evoluzione degli organi rappresentativi e legali, la sede, la Partita IVA, il Codice fiscale, la titolarità di diritti o la disponibilità di beni strumentali;
- 3) Dati sensibili, ai sensi dell'art. 4, comma 1, lett. d) del d.lgs. n. 196 del 2003;
- 4) Dati giudiziari, ai sensi dell'art. 4, comma 1, lett. e) del d.lgs. n. 196 del 2003;
- 5) Dati inerenti il livello di istruzione e culturale nonché relativi all'esito di scrutini, esami, piani educativi individualizzati differenziati;
- 6) Dati inerenti le condizioni economiche e l'adempimento degli obblighi tributari;
- 7) Dati riferibili a procedimenti giudiziari, pendenti in qualsiasi grado, o pregressi, di natura civile, amministrativa, tributaria, presso autorità giurisdizionali italiane o estere, diversi da quelli rientranti nell'art. 4 comma 1, lett. e) del d.lgs. n. 196 del 2003;
- 8) Dati atti a rilevare la presenza presso l'istituzione scolastica dei destinatari dell'offerta formativa ovvero dei familiari nonché del personale coinvolto, a qualsiasi titolo, nella somministrazione di tale offerta;
- 9) Dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque;
- 10) Dati inerenti negoziazioni e relative modalità di pagamento rispetto a forniture di beni, servizi o di opere, ovvero proposte ed offerte inerenti le medesime negoziazioni;
- 11) Dati inerenti la fornitura e le modalità di pagamento riguardo ad attività professionale a fini formativi;
- 12) Dati contabili e fiscali;
- 13) Dati inerenti la titolarità di diritti, il possesso o la detenzione di beni mobili registrati, mobili o immobili;
- 14) Dati detenuti in applicazione di disposizioni di origine nazionale o comunitaria, atti o provvedimenti amministrativi, fonti contrattuali.

3. RESPONSABILE TRATTAMENTO DATI

L'ente titolare del trattamento dei dati ha designato, mediante autonomo provvedimento (allegato al presente Documento) quale Responsabile ai sensi dell'art. 29 del d.lgs. n. 196 del 2003 la Dott.ssa Maria Stella Pitocco, nata a Roma il 15/10/67, preposto alle funzioni di DSGA, in considerazione della esperienza, capacità ed affidabilità espressa dal medesimo, tale da offrire idonea garanzia del pieno rispetto delle disposizioni in materia di trattamento.

Il suddetto Responsabile del trattamento ha ricevuto adeguate istruzioni riguardo:

- a) all'individuazione ed adozione delle misure di sicurezza da applicare nell'ambito dell'istituzione scolastica, al fine di salvaguardare la riservatezza, l'integrità, la completezza e la disponibilità dei dati trattati;
- b) all'esigenza di provvedere, mediante atto scritto, all'individuazione delle unità legittimate al trattamento, per mezzo dei singoli preposti, ovvero di singoli incaricati, ai sensi dell'art. 30 del d.lgs. n. 196 del 2003, deputati ad operare sotto la diretta autorità del responsabile, attenendosi alle istruzioni impartite, fermo restando l'obbligo gravante sul responsabile, di vigilare sul rispetto delle misure di sicurezza adottate.
- c) all'esigenza di verificare che gli obblighi di informativa siano stati assolti correttamente, ovvero che sia stato conseguito il consenso degli interessati;
- d) all'obbligo di collaborare con il titolare nell'adempiere alle richieste avanzate dal Garante per la protezione dei dati personali ovvero alle autorità investite dei poteri di controllo;
- e) all'attribuzione della competenza a elaborare e sottoscrivere notificazioni al Garante per la protezione dei dati personali;
- f) all'obbligo di osservare e far osservare il divieto di comunicazione e diffusione dei dati personali comunque trattati da parte dell'istituzione scolastica;
- g) all'obbligo, ovvero a proporre soluzioni organizzative che consentano un ampliamento dei livelli di sicurezza

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

Tali incaricati, in particolare, sono stati formalmente edotti in merito alla circostanza che:

- a) il trattamento e la conservazione dei dati deve avvenire esclusivamente in modo lecito e proporzionato alle funzioni istituzionali, nel rispetto della riservatezza;
- b) la raccolta, registrazione ed elaborazione dei dati, mediante strumento informatico o cartaceo, deve essere limitata alle finalità istituzionali;
- c) integra onere dell'incaricato la correzione od aggiornamento dei dati posseduti, l'esame della loro pertinenza rispetto alle funzioni
- d) integra inosservanza delle istruzioni la comunicazione, effettuata in qualsiasi maniera dei dati in possesso, con eccezione del caso che il destinatario sia l'interessato alle stesse, ovvero altri soggetti legittimati ad ricevere dette comunicazioni.

L'ambito dei trattamenti autorizzati ai singoli incaricati è suscettibile di aggiornamento periodico.

A tutti gli incaricati destinati al trattamento di dati mediante strumento elettronico, sono state conferite credenziali di autenticazioni (art. 34, comma 1, lett. b) mediante parola chiave, conformi alle caratteristiche indicate nell'allegato B. Con atto allegato al presente documento è stato designato l'incaricato della custodia delle copie di credenziali di autenticazione nonché della funzione di verifica del loro aggiornamento periodico ovvero della corretta utilizzazione.

Le suddette credenziali sono disattivate automaticamente dal gestore della rete periodicamente, ovvero in tutti i casi di mancata utilizzazione per almeno 6 mesi.

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

4. AMBITO DEI TRATTAMENTI.

Attesa la dislocazione dell'istituzione scolastica in più edifici, si precisano le modalità del trattamento dei dati nei vari uffici e sedi, mediante strumenti elettronici, secondo le modalità precisate nella tabella sottostante.

Tabella 2 Elenco dei trattamenti: informazioni di base

| Struttura deputata al trattamento | Natura dei dati trattati | | Struttura di riferimento | Altre strutture (anche esterne) che concorrono al trattamento | Descrizione degli strumenti utilizzati |
|---|--------------------------|------------|--------------------------|---|--|
| | Sensibili | Giudiziari | | | |
| Ufficio Protocollo | Sensibili | Giudiziari | Segreteria | Ditta esterna, limitatamente alle esigenze di manutenzione e/o riparazione dei p.c interni e/o del server | Pc interno più server interno |
| Ufficio personale | Sensibili | Giudiziari | Segreteria | Ditta esterna, limitatamente alle esigenze di manutenzione e/o riparazione dei p.c interni e/o del server | Pc interno più server interno |
| Servizi amministrativi | Sensibili | | Segreteria amm.va | Ditta esterna, limitatamente alle esigenze di manutenzione e/o riparazione dei p.c interni e/o del server | Pc interno più server interno |
| Servizi inerenti l'offerta formativa e servizi strumentali agli organi collegiali | Sensibili | Giudiziari | Segreteria | Ditta esterna, limitatamente alle esigenze di manutenzione e/o riparazione dei p.c interni e/o del server | Pc interno più server interno |
| | | | | | |

Il trattamento dei dati avviene attraverso modalità diverse: strumenti elettronici, interni (P.C.) ovvero collegati in rete fra loro, e/o mediante collegamenti alla rete intranet ed alla RUPA, e/o alla rete internet. Con riferimento alla gestione dei dati mediante rete ministeriale e RUPA, l'Istituzione scolastica declina ogni responsabilità, operando come semplice utente, non essendo in grado di intervenire sulla gestione delle informazioni ivi contenute e gestite.

Con riferimento all'ubicazione fisica dei supporti di memorizzazione delle copie di sicurezza, l'Istituzione scolastica, tenendo conto dell'analisi di cui al punto 5, ha ritenuto di provvedere alla custodia presso la cassaforte dell'Ufficio di Segreteria, riservando l'accesso a tali supporti alla Prof.ssa Giuliana Santagata.

La tabella seguente riassume il quadro dei trattamenti secondo modalità e tipologia, precisando l'ubicazione dei supporti di memorizzazione.

Tabella 3 Elenco dei trattamenti: descrizione degli strumenti utilizzati

| IDENTIFICATIVO DEL TRATTAMENTO | EVENTUALI BANCHE DATI DI SUPPORTO | UBICAZIONE FISICA DEI SUPPORTI DI MEMORIZZAZIONE E DELLE COPIE DI SICUREZZA | TIPOLOGIA DI DISPOSITIVI DI ACCESSO | TIPOLOGIA DI INTERCONNESSIONE |
|--------------------------------|---|---|-------------------------------------|-------------------------------|
| Ufficio Protocollo | Ruoli del personale in formato elettronico | Nei locali dell'Istituzione scolastica siti al Piano | Pc | Rete locale e Internet |
| Ufficio personale | Ruoli del personale in formato elettronico; Archivio del personale (N.B. le tabelle realizzate con excel recano l'indicazione delle assenze per festività religiose non cattoliche e/o condanne penali, appartenenza di uno o più dipendenti a categorie protette con handicap, etc.) | Come sopra | Pc | Rete locale e Internet |
| Servizi amministrativi | Archivio delle imprese fornitrici di servizi e/o prestazioni. Archivio contenuto negli elaboratori sottoposti a revisione o manutenzione da parte di tecnici, anche esterni, incaricati degli interventi (sia in caso di trasporto dell'elaboratore all'esterno dell'ente, presso i locali della ditta, sia in caso di intervento sul posto, cioè nei locali dell'istituzione scolastica) | Come sopra | Pc | Rete locale e Internet |
| Servizi inerenti | Destinatari | Come sopra | Pc oppure Pc e | Rete locale e |

| | | | | |
|--|---|--|--------|----------|
| l'offerta formativa e servizi strumentali agli organi collegiali | dell'offerta formativa con caratterizzazione religiosa, economica, sociale, sanitaria (cfr. Modello Excel e relativo "modello di previsione h") | | server | Internet |
|--|---|--|--------|----------|

5. ANALISI DEI RISCHI INCOMBENTI SUI DATI.

L'Istituzione scolastica ha proceduto ad una ricognizione dei rischi che potrebbero comportare una distruzione, sottrazione, perdita, trattamento abusivo dei dati, di origine dolosa, colposa, ovvero meramente fortuito, in grado di recare pregiudizio ai dati personali trattati.

Le fonti di rischio sono state accorpate in:

1) Comportamenti degli operatori.

Sottrazione di credenziali di autenticazione; comportamenti imperiti, imprudenti o negligenti dei soggetti legittimati al trattamento dei dati; comportamenti dolosi dei soggetti legittimati; errori materiali.

2) Eventi relativi agli strumenti.

Danno arrecato da virus informatici e/o da hackers, mediante interventi precedenti all'aggiornamento degli strumenti di contrasto attivati (software e firewall), spamming o tecniche di sabotaggio. Malfunzionamento, indisponibilità o usura fisica degli strumenti. Accessi abusivi negli strumenti elettronici. Intercettazione dei dati in occasione di trasmissione in rete.

3) Eventi relativi al contesto fisico-ambientale.

Distruzione o perdita di dati in conseguenza di eventi incontrollabili (terremoto) ovvero, seppur astrattamente preventivabili (incendi o allagamenti) di origine fortuita, dolosa o colposa, per i quali non è possibile apprestare cautele. Guasti a sistemi complementari, quale la mancata erogazione di energia elettrica per lunghi periodi di tempo, in grado di pregiudicare la climatizzazione dei locali. Furto o danneggiamento degli strumenti elettronici di trattamento dei dati, in orario diverso da quello di lavoro. Accesso non autorizzato da parte di terzi – interni o esterni all'istituzione scolastica – mediante uso abusivo di credenziali di autenticazione, in funzione di danneggiamento o sottrazione dei dati. Errori umani nell'attivazione degli strumenti di protezione.

I suddetti rischi sono stati ripartiti in classi di gravità, tenendo conto della concreta possibilità di realizzazione presso l'istituzione scolastica, adottando la seguente scansione:

A= alto B = basso EE = molto elevato M = medio MA = medio-alto MB = medio-basso

La tabella seguente sintetizza i principali eventi potenzialmente dannosi per la sicurezza dei dati, valutandone le possibili conseguenze e stimandone la gravità, ponendoli altresì in correlazione con le misure di sicurezza previste.

Tabella 4 Analisi dei rischi

| EVENTO | | IMPATTO SULLA SICUREZZA DEI DATI | | RIF. MISURE DI AZIONE |
|---------------------------------------|---|---|-----------------|---|
| | | DESCRIZIONE | GRAVITÀ STIMATA | |
| COMPORAMENTI DEGLI OPERATORI | Furto di credenziali di autenticazione | Accesso altrui non autorizzato | M | Vigilanza sul rispetto delle istruzioni impartite |
| | Carenza di consapevolezza, disattenzione o incuria | Dispersione, perdita e accesso altrui non autorizzato | M | Formazione e flusso continuo di informazione |
| | Comportamenti sleali o fraudolenti | Dispersione, perdita e accesso altrui non autorizzato | M | Vigilanza sul rispetto delle istruzioni impartite |
| | Errore materiale | Dispersione, perdita e accesso altrui non autorizzato | M | Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione |
| EVENTI RELATIVI AGLI STRUMENTI | Azione di virus informatici o di codici malefici | Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; | EE | Adozione di idonei dispositivi di protezione |
| | Spamming o altre tecniche di sabotaggio | Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | EE | Adozione di idonei dispositivi di protezione |
| | Malfunzionamento, indisponibilità o degrado degli strumenti | Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | MA | Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico |

| | | | | |
|------------------------------------|---|--|-----------|--|
| | Accessi esterni non autorizzati | Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | MA | Adozione di idonei dispositivi di protezione |
| | Intercettazione di informazioni in rete | Dispersione di dati; accesso altrui non autorizzato | MA | Adozione di idonei dispositivi di protezione |
| EVENTI RELATIVI AL CONTESTO | Accessi non autorizzati a locali/reparti ad accesso ristretto | Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | M | Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati |
| | Asportazione e furto di strumenti contenenti dati | Dispersione e perdita di dati, di programmi e di elaboratori; accesso altrui non autorizzato | MB | Protezione dei locali e dei siti di ubicazione degli elaboratori e dei supporti di memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati |
| | Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria | Perdita di dati, dei programmi e degli elaboratori | M | Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione |

| | | | | |
|--|---|---|----------|---|
| | Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.) | Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | A | Attività di controllo, assistenza e manutenzione periodica |
| | Errori umani nella gestione della sicurezza fisica | Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | M | Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione |

6. MISURE ADOTTATE PER GARANTIRE L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI, NONCHÉ LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITÀ.

Sulla scorta della ricognizione dei rischi sopra rappresentata, l'istituzione scolastica ha provveduto ad apprestare e/o introdurre strumenti di tutela, ovvero a prevedere successive, e più incisive, misure di sicurezza. La tabella seguente sintetizza le misure di sicurezza in essere, corredate da indicazioni di dettaglio.

Tabella 5 Le misure di sicurezza adottate o da adottare

| MISURA | RISCHIO CONTRASTATO | STRUTTURA INTERESSATA | EVENTUALE BANCA DATI INTERESSATA | MISURA GIÀ IN ESSERE | PERIODICITÀ E RESPONSABILITÀ DEI CONTROLLI |
|---|--|-----------------------|----------------------------------|---|---|
| Preventiva, di contrasto, di contenimento degli effetti | Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | Ufficio Protocollo | Relativo archivio | Antivirus, Firewall e credenziali di autenticazione | Bimestrale; responsabile pro tempore del servizio |

| | | | | | |
|---|--|--------------------------------------|-------------------|---|--|
| Preventiva, di contrasto, di contenimento degli effetti | Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | Ufficio personale | Relativo archivio | Antivirus, Firewall e credenziali di autenticazione | Bimestrale; responsabile pro tempore del servizio e, per la parte di competenza, della ditta esterna |
| Preventiva, di contrasto, di contenimento degli effetti | Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | Servizi amministrativi | Relativo archivio | Antivirus, Firewall e credenziali di autenticazione | Bimestrale; responsabile pro tempore del servizio |
| Preventiva, di contrasto, di contenimento degli effetti | Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | Servizi inerenti l'offerta formativa | Relativo archivio | Antivirus, Firewall e credenziali di autenticazione | Bimestrale; responsabile pro tempore del servizio |

| | | | | | |
|---|--|--|-------------------|---|---|
| Preventiva, di contrasto, di contenimento degli effetti | Dispersione, perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi | Servizi strumentali agli organi collegiali | Relativo archivio | Antivirus, Firewall e credenziali di autenticazione | Bimestrale; responsabile pro tempore del servizio |
| Data: | | | | | |

7. CRITERI E MODALITÀ PER IL RIPRISTINO DELLA DISPONIBILITÀ DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita, è stata definita una procedura di periodica esecuzione di copie di sicurezza dei dati trattati. Sono state perciò acquisite licenze di uso per software antivirus, nonché sistemi di firewall con verifica di idoneità e costante aggiornamento. In ogni caso si osserva che l'istituzione scolastica dispone di un sistema di controllo degli accessi ai locali. I documenti sono anche conservati in copia cartacea presso locali dell'istituzione scolastica non accessibili ai terzi e dotati di adeguati strumenti di protezione (armadi con serrature, stanze protette da inferriate).

Sinteticamente è possibile rappresentare la seguente procedura di copia, verifica e ripristino dei dati per ogni p.c. o terminale di collegamento a server

Tabella 6 Procedure di copia, verifica e ripristino per ogni singola unità contenente dati

| STRUTTURA IN POSSESSO DI P.C. O COLLEGAMENTO A SERVER | APPLICATIVO | SISTEMA OPERATIVO | SUPPORTI MAGNETICI | PROCEDURA DI COPIA | PROCEDURA DI VERIFICA | RIPRISTINO |
|---|-------------|--------------------|--------------------|---|---|---|
| Segreteria Dirigente scolastico | Office | Server Windows2000 | Cassette Tipo DAT | Procedura di back-up Windows2000 server | Procedura di back-up Windows2000 server | Procedura di back-up Windows2000 server |
| Ufficio personale | Office | Server Windows2000 | Cassette Tipo DAT | Procedura di back-up Windows2000 server | Procedura di back-up Windows2000 server | Procedura di back-up Windows2000 server |
| Servizi amministrativi | Office | Server Windows2000 | Cassette Tipo DAT | Procedura di back-up Windows2000 server | Procedura di back-up Windows2000 server | Procedura di back-up Windows2000 server |
| Servizi inerenti l'offerta formativa | Office | Server Windows2000 | Cassette Tipo DAT | Procedura di back-up Windows2000 server | Procedura di back-up Windows2000 server | Procedura di back-up Windows2000 server |
| Servizi strumentali agli | Office | Server Windows2000 | Cassette Tipo DAT | Procedura di back-up | Procedura di back-up | Procedura di back-up |

| | | | | | | |
|-------------------|--|--|--|--------------------|--------------------|--------------------|
| organi collegiali | | | | Windows2000 server | Windows2000 server | Windows2000 server |
| Data | | | | | | |

Con riferimento invece al contenuto ed alle competenze in tema di copia, verifica e ripristino, le soluzioni organizzative adottate presso l'istituzione scolastica sono sintetizzate nella seguente tabella

Tabella 7 Salvataggio dei dati

| SALVATAGGIO | | CRITERI INDIVIDUATI PER IL SALVATAGGIO | UBICAZIONE DI CONSERVAZIONE DELLE COPIE | STRUTTURA OPERATIVA INCARICATA DEL SALVATAGGIO |
|---|--|--|--|--|
| STRUTTURA | DATI SENSIBILI O GIUDIZIARI CONTENUTI | | | |
| Segreteria Dirigente scolastico | | Salvataggio dati periodico | Locale Segreteria , piano terra, con serratura con chiavi distribuite fra i soli autorizzati | Responsabile pro tempore del servizio |
| Ufficio personale | - Stato di salute (dispense dal servizio, aspettative) - adesione a sindacati - origine razziale o etnica - confessione religiosa | Salvataggio dati periodico. | Locale Segreteria, piano terra, con serratura con chiavi distribuite fra i soli autorizzati; | Responsabile pro tempore del servizio |
| Servizi amministrativi | - dati giudiziari inerenti imprese interessate ad attività negoziali | Salvataggio dati periodico | Locale Segreteria, piano terra , con serratura con chiavi distribuite fra i soli autorizzati; | Responsabile pro tempore del servizio |
| Servizi inerenti l'offerta formativa e servizi strumentali agli organi collegiali | - Stato di salute -adesione a sindacati - origine razziale o etnica - confessione religiosa | Salvataggio dati periodico. | Locale sito Segreteria, pianoterra con serratura con chiavi distribuite fra i soli autorizzati | Responsabile pro tempore del servizio |
| Data: | | | | |

Con riferimento alle procedure di ripristino, l'Istituzione scolastica ha adottato le seguenti modalità

Tabella 8 Ripristino dei dati

| RIPRISTINO (in seguito a distruzione o danneggiamento) | | |
|---|--|---|
| DATA BASE/ARCHIVIO | SCHEDA OPERATIVA | PIANIFICAZIONE DELLE PROVE DI RIPRISTINO |
| Ufficio protocollo | Viene effettuato un back up dei dati trattati e dei documenti presenti sull'HD su diverse copie di supporti che vengono conservate in più locali con serratura, ma sempre all'interno della sede dell'istituzione scolastica di Via Albergotti | Trimestrale |
| Ufficio personale | Come sopra | Trimestrale |
| Servizi amministrativi | Come sopra | Trimestrale |
| Servizi inerenti l'offerta formativa | Come sopra | Trimestrale |
| Servizi strumentali agli organi collegiali | Come sopra | Trimestrale |
| Data: | | |

8. PROGRAMMA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO.

L'istituzione scolastica intende aderire alle iniziative formative organizzate dalla direzione regionale del Ministero dell'Istruzione dell'Università e della Ricerca Scientifica, tenendo anche conto dell'economicità di un'azione organizzata su base regionale, rispetto ad una gestione in proprio delle attività formative. L'istituzione opera integrale rinvio alla programmazione della Direzione regionale, riservandosi comunque di agire in via suppletiva, qualora, per ragione organizzative od economiche, non sia possibile far partecipare il proprio personale alle attività di formazione necessarie per adempiere alle prescrizioni ordinamentali. A tal fine è stata designata, con atto allegato al presente documento, la persona incaricata di curare l'effettiva esecuzione dell'attività formativa da parte del personale coinvolto.

Tabella 9 Pianificazione degli interventi formativi

| CORSO DI FORMAZIONE (OGGETTO) | DESCRIZIONE SINTETICA DELL'OBIETTIVO FORMATIVO | CLASSI DI INCARICO INTERESSATE | NUMERO DI INCARICATI INTERESSATI | NUMERO DI INCARICATI GIÀ FORMATI/DA FORMARE NEL CORSO DELL'ANNO | CALENDARIO |
|---|--|--|---|--|---------------------------------------|
| L'adempimento dell'obbligo di aggiornamento del DPS | Porre in condizione il personale competente di adempiere entro il 31.6.2005 all'obbligo di aggiornamento del DPS | Tutto il personale segreteria scolastica | | | Concordato con la direzione regionale |

| | | | | | |
|---|--|--|--|--|---------------------------------------|
| Quadro riepilogativo degli adempimenti e degli obblighi in materia di privacy (ivi incluse le misure di sicurezza per gli archivi cartacei) | Mantenimento del richiesto grado di conoscenza dell'intero impianto della normativa in materia di privacy, anche ai fini delle misure di sicurezza da adottare per gli archivi cartacei. | Tutto il personale segreteria scolastica | | | Concordato con la direzione regionale |
| Privacy e diritto di accesso nelle istituzioni scolastiche | Fornire un quadro coordinato dei diritti (di accesso e alla riservatezza) riconosciuti all'utenza dalla vigente legislazione, in rapporto ai doveri gravanti sulle strutture scolastiche | Tutto il personale segreteria scolastica | | | Concordato con la direzione region |
| Esame della casistica ricorrente nell'attività di ufficio, alla luce delle sentenze del giudice amministrativo e dei pronunciamenti del Garante | Aggiornare il personale sull'evoluzione dell'interpretazione della normativa intervenuta nel corso dell'anno | Tutto il personale segreteria scolastica | | | Concordato con la direzione region |
| Data: | | | | | |

9. TRATTAMENTI DI DATI PERSONALI SENSIBILI O GIUDIZIARI CON STRUMENTI ELETTRONICI AFFIDATI ALL'ESTERNO.

L'Istituzione scolastica, ha proceduto alla esternalizzazione di taluni trattamenti, secondo modalità conformi a quanto previsto dal d.lgs. n. 196 del 2003, procedendo alla nomina di un soggetto esterno quale responsabile del trattamento, limitatamente ai dati e alle operazioni necessari per lo svolgimento delle attività conferite. A tal fine l'Istituzione scolastica ha imposto le cautele indicate in calce alla tabella che segue, affinché il soggetto destinatario adotti le misure di sicurezza richieste dal Codice, ivi incluso il relativo all. B.

Per i soggetti indicati nella seguente tabella, l'atto di nomina è allegato al presente DPS (all. n. 3).

Tabella 10 Trattamenti affidati all'esterno

| ATTIVITÀ ESTERNALIZZATA COMPORTANTE TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI | DESCRIZIONE SINTETICA | DATI PERSONALI, SENSIBILI O GIUDIZIARI INTERESSATI | SOGGETTO ESTERNO | DESCRIZIONE DEI CRITERI PER L'ADOZIONE DELLE MISURE |
|--|--|--|--|--|
| | Necessario per lo svolgimento delle attività strumentali finalizzate all'installazione e al buon funzionamento degli elaboratori, dei programmi e degli altri strumenti elettronici in dotazione agli uffici | | Ditta esterna (ISMEDA) di cui al contratto in essere, allegato al presente DPS, come integrato dall'allegato atto di nomina a responsabile dei relativi trattamenti | Vincolo contrattuale, a carico del fornitore esterno, a tenere i comportamenti descritti in calce alla presente tabella. |
| Data: | | | | |

10. VINCOLI CONTRATTUALMENTE ASSUNTI DAL FORNITORE ESTERNO AI FINI DELLA SICUREZZA DEI DATI

L'Istituzione scolastica ha affidato all'esterno (soc. **ISMEDA**), nei termini risultanti dalla sopraindicata tabella, i trattamenti di dati personali sensibili o giudiziari, effettuato con strumenti elettronici, previa assunzione da parte dell'affidatario – nell'ambito dello stesso contratto con cui viene realizzato l'affidamento o con atto aggiuntivo – degli impegni derivanti dalle seguenti dichiarazioni:

1. di essere consapevole che i dati che tratterà nell'espletamento dell'incarico ricevuto, sono dati personali e, come tali sono soggetti all'applicazione del codice per la protezione dei dati personali;
2. di ottemperare agli obblighi previsti dal Codice per la protezione dei dati personali;
3. di adottare le istruzioni specifiche ricevute per il trattamento dei dati personali e di integrarle nelle procedure già in essere;
4. di impegnarsi a relazionare annualmente sulle misure di sicurezza adottate e di avvertire (allertare) immediatamente il proprio committente in caso di situazioni anomale o di emergenze;
5. di riconoscere il diritto del committente a verificare periodicamente l'applicazione delle norme di sicurezza adottate.

11. ATTI E DOCUMENTI NON IN FORMATO ELETTRONICO, ARCHIVI CARTACEI

I trattamenti di dati personali con strumenti diversi da quelli elettronici sono effettuati dagli incaricati seguendo le istruzioni scritte ad essi impartite con il documento di cui all'allegato 1, finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. L'aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati ha carattere annuale. Gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti. I medesimi atti e documenti sono controllati e custoditi dagli incaricati

fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

L'accesso agli archivi contenenti dati sensibili o giudiziari è consentito solamente alle persone preventivamente autorizzate.

12. SISTEMA DI AUTORIZZAZIONE.

Al momento, considerata la forte carenza di personale e le esigenze organizzative dell'ente, per il cui ordinario funzionamento è indispensabile assicurare una certa interscambiabilità funzionale degli incaricati, non è stato adottato un sistema di autorizzazione.


13. OBBLIGO DI AGGIORNAMENTO PERIODICO DEL DPS

Il presente documento programmatico sulla sicurezza è sottoposto a revisione annuale nella sua interezza, entro la scadenza del 31 marzo di ciascun anno, come previsto dalla regola 19 del Disciplinare tecnico di cui all'allegato B) al D.Lgs. 196/03, in relazione al disposto dell'art. 34, lettera g) del decreto stesso.

Gli allegati al presente documento ne formano parte integrante.

Il presente documento è aggiornato al 31/12/2006.

IL TITOLARE DEL TRATTAMENTO

The image shows a circular official seal on the left, which is the emblem of the Italian Ministry of Education, University and Scientific Research (MUR). To the right of the seal, the text reads "Il Dirigente Scolastico (Prof. Maurizio De Renzi)" followed by a handwritten signature in black ink.

IL RESPONSABILE DEL TRATTAMENTO
Dott.ssa M. Stella Pitocco