ISTITUTO SUPERIORE "V. Capirola" BSIS00900X

Piazza C. Battisti, 7/ 8 25124 Leno (BS)

Documento Programmatico sulla Sicurezza

ai sensi del D.L. n.196, 30/06/2003 "Codice in materia di protezione dei dati personali"

Titolo documento:	**Documento Programmatico sulla Sicurezza (DPS)**
Codice documento:	**DPS Istituto Superiore " V. Capirola" di Leno**
Nome file:	**DPS_CAPIROLA2011**
Stato documento:	**Revisione 2011**
Emesso	**24 Marzo 2011**
Protocollo	**1848 C24**
Validità	**Fino alla successiva revisione non oltre il 31 marzo 2012**

Approvato da:

RESPONSABILI DPS	IN QUALITÀ DI	FIRMA
Dirigente Scolastico	Titolare	
DSGA	Responsabile del Trattamento	

Indice del documento:

1 Introduzione

Il Decreto legislativo 30 giugno 2003, n. 196 – Codice in materia di protezione dei dati personali, di seguito denominato "Codice", è istituito per garantire che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Riconosciuta la necessità da parte dell' Istituto Superiore " V. Capirola" di Leno di trattare dati personali di varia natura, il Codice prescrive che i sistemi informativi e i programmi informatici siano configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Il Codice prescrive inoltre che i dati personali oggetto di trattamento siano custoditi e controllati anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediante l'adozione di idonee e preventive misure di sicurezza, i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta (art. 31 – Obblighi di sicurezza).

A questo scopo sono indicate una serie di misure minime di sicurezza da adottare nei modi descritti attualmente dall'allegato B del Codice (Disciplinare tecnico in materia di misure minime di sicurezza) che riguardano, per quanto attiene i trattamenti effettuati con strumenti elettronici:

- autenticazione informatica;
- adozione di procedure di gestione delle credenziali di autenticazione;
- utilizzazione di un sistema di autorizzazione;
- aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici;
- protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici;
- adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;
- tenuta di un aggiornato documento programmatico sulla sicurezza;

Per ciò che concerne i trattamenti effettuati senza l'ausilio di strumenti elettronici, il Codice prescrive di:

- aggiornare periodicamente l'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
- prevedere una serie di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
- prevedere una serie di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina delle modalità di accesso finalizzata all'identificazione degli incaricati.

L'analisi della situazione attuale riguardo i punti elencati e la previsione di idonee misure tecniche e organizzative atte a rispettarne la lettera e lo spirito saranno quindi parte integrante e scopo di questo documento programmatico.

Il Documento Programmatico sulla Sicurezza è, in sostanza, una rappresentazione attenta e responsabile dei rischi e delle misure da adottare per prevenirne le conseguenze. Ai fini della redazione e dei successivi aggiornamenti è stata e sarà necessaria una attenta disamina delle disposizioni interne alla struttura previste per il trattamento dei dati personali.

Particolare attenzione è stata rivolta ai trattamenti di dati sensibili e giudiziari, agli strumenti tramite i quali vengono effettuati e alla gestione organizzativa delle aree in cui vengono svolti tali trattamenti.

Fondamentale è stata quindi la preventiva analisi dei rischi, condotta analizzando anche aspetti tecnici e organizzativi più ampi rispetto alle prescrizioni legislative.

1.1 Scopo del documento

Il presente Documento Programmatico Sulla Sicurezza (per brevità in seguito denominato anche DPS) dell' Istituto Superiore " V. Capirola" di Leno è adottato ai sensi dell'art. 34 del decreto legislativo n. 196 del 30 giugno 2003, "Codice in materia di protezione dei dati personali", per definire le politiche di sicurezza in materia di trattamento di dati personali ed i criteri organizzativi per la loro attuazione. Nel presente Documento Programmatico Sulla Sicurezza vengono definiti i criteri tecnici e organizzativi per garantire la sicurezza dei dati personali trattati dalla scuola, descrivendo come prescritto dal *Disciplinare tecnico in materia di misure minime di sicurezza* (allegato B del Codice):

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento dei dati o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni;

- la previsione degli interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Nella redazione del presente documento, oltre a quanto prescritto dal D.L. 196/03, i redattori hanno tenuto presenti i seguenti obiettivi:

- avere una visione il più possibile completa e dettagliata del grado di esposizione a varie tipologie di rischi del patrimonio informativo del Istituto Superiore " V. Capirola" di Leno
- individuare e mettere in atto non solo le misure minime di sicurezza prescritte dal Codice e dal Disciplinare tecnico, ma, dove possibile, le misure idonee (organizzative, tecnologiche, logistiche, normative e procedurali) atte a garantire la protezione dei dati personali;
- assicurare che la gestione dei dati personali e più in generale di tutti i dati necessari all'attività dell'Istituto avvenga con un ragionevole livello di sicurezza e riservatezza nel corso di tutte le modalità di trattamento, comprese quelle che utilizzano strumenti diversi da quelli elettronici.

1.2 Struttura del documento

In applicazione a quanto prescritto dal Codice e alle esigenze di esposizione delle problematiche, il presente documento si articola nelle seguenti sezioni principali:

- Individuazione dei trattamenti in atto di cui la scuola è titolare
- Strutture per la gestione dei dati
- Definizione dei compiti e delle responsabilità
- Analisi dei rischi che incombono sui dati
- Definizione delle misure di sicurezza
- Piano di verifica
- Piano di formazione e sensibilizzazione

Ciascuna sezione principale potrà comprendere sottosezione articolate che descrivano nel dettaglio gli argomenti trattati.

1.3 Aggiornamento

Il presente documento è soggetto a revisione annuale, da compiersi entro il 31 marzo, come disposto dalla normativa vigente.

1.4 Contesto normativo di riferimento

- Decreto legislativo n. 196 del 30 giugno 2003 Codice in materia di protezione dei dati personali.
- Decreto legge n. 354 del 24 dicembre 2003 Interventi per l'amministrazione della giustizia negli art. 4 e 5 Modifiche agli articoli 181 e 183 del d.l. 196 del 30 giugno 2003.
- Legge n. 547 del 23 dicembre 1993 Modificazioni ed integrazioni del codice penale e del codice di procedura penale in tema di criminalità informatica.
- Decreto legislativo n. 518 del 29 dicembre 1992 Attuazione della direttiva 91/250/CEE relativa alla tutela giuridica dei programmi per elaboratore e Legge n. 248 del 18 agosto 2000 Nuove norme di tutela del diritto d'autore.

1.5 Atti dell' Istituto Superiore " V. Capirola" di Leno relativi alla privacy

- Individuazione delle banche dati informatizzate e degli archivi cartacei contenenti dati soggetti a tutela della privacy. Individuazione del titolare e dei responsabili del trattamento degli stessi dati.
- Informativa all'utenza. (allegato B e B bis)
- richiesta diffusione esiti scolastici (allegato H)

1.6 Definizioni

Ai fini del presente documento si adottano le definizioni riportate all'art. 4 del Codice, indicando con:

"**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;

"**dato personale**", 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;

"**titolare**", la persona fisica, la persona giuridica, la pubblica amministrazione e qualsiasi altro ente, associazione od organismo cui competono, anche unitamente ad altro titolare, le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, ivi compreso il profilo della sicurezza;

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

"**incaricati**", le persone fisiche autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile;

"**interessato**", la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali;

"**comunicazione**", il dare conoscenza dei dati personali a uno o più soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dello Stato, dal responsabile e dagli incaricati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione;

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

"**dato anonimo**", il dato che in origine, o a seguito di trattamento, non può essere associato ad un interessato identificato o identificabile;

"**banca dati**", qualsiasi complesso organizzato di dati personali, ripartito in una o più unità dislocate in uno o più siti;

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

"**misure minime**", il complesso delle misure tecniche, informatiche, organizzative, logistiche e procedurali di sicurezza che configurano il livello minimo di protezione richiesto in relazione ai rischi previsti nell'articolo 31;

"**strumenti elettronici**", gli elaboratori, i programmi per elaboratori e qualunque dispositivo elettronico o comunque automatizzato con cui si effettua il trattamento;

"**autenticazione informatica**", l'insieme degli strumenti elettronici e delle procedure per la verifica anche indiretta dell'identità;

"**credenziali di autenticazione**", i dati ed i dispositivi, in possesso di una persona, da questa conosciuti o ad essa univocamente correlati, utilizzati per l' autenticazione informatica;

"**password**" o "**parola chiave**", componente di una credenziale di autenticazione associata ad una persona ed a questa nota, costituita da una sequenza di caratteri o altri dati in forma elettronica;

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

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

2 Individuazione dei trattamenti

Tutti i trattamenti in atto nell'istituzione scolastica sono effettuati in relazione a funzioni e compiti ad essa attribuiti, delegati o conferiti dalla normativa statale, regionale e comunitaria, funzioni previste dai regolamenti, a funzioni svolte in attuazione di convenzioni, accordi di programma, intese e sulla base di strumenti di programmazione negoziata previsti dalla legislazione vigente, a funzioni collegate all'accesso ed all'erogazione dei servizi resi dall'Istituto agli utenti, a funzioni svolte in attuazione di Contratti collettivi nazionali e decentrati in materia di pubblico impiego nonché a quelle inerenti all'organizzazione dell'Amministrazione ed allo sviluppo dell'attività amministrativa, nei suoi vari profili.

La gestione delle informazioni confluenti nelle banche dati e negli archivi dell'Istituto è realizzata nel rispetto dei principi e dei criteri che regolano il trattamento dei dati personali. Le ripartizioni dell'Istituto provvedono periodicamente e comunque con cadenza almeno annuale a verificare e censire i trattamenti di dati personali, al fine di rilevare eventuali specificità degli stessi e di definire adeguate modalità per la corretta gestione delle informazioni.

Alla data di revisione di questo documento, l' Istituto Superiore " V. Capirola" di Leno ha provveduto ad avviare il censimento di tutti i trattamenti e di tutte le banche dati, elettroniche e cartacee, presenti presso le proprie ripartizioni.

Tale rilevazione ha lo scopo di individuare le tipologie di dati gestiti, le fasi di cui si compone ciascun trattamento, le misure di sicurezza attivate e da attivare a protezione dei dati, l'interconnessione con altre banche dati interne od esterne, la necessità di comunicazione o diffusione dei dati raccolti, chiarendo inoltre sulla base di quali indicazioni normative o di quali esigenze organizzative interne detti trattamenti vengono effettuati, nonché di valutare l'eventuale sussistenza di trattamenti non attinenti le finalità istituzionali dell'Istituto.

L'elenco dei trattamenti effettuati, nello specifico è riportato nell'allegato A.

Elenco dei trattamenti di dati personali e strutture preposte ai trattamenti sintesi.

ID TRATTAM.	DESCIZIONE SINTETICA	STRUTTURA OPERATIVA PRINCIPALE	ALTRE STRUTTURE CONCORRENTI QUANDO NECESSARIE
TD01	Selezione e reclutamento a tempo indeterminato e determinato del rapporto di lavoro del personale	Dirigente Segreteria	Collaboratori del dirigente Collaboratori Scolastici Responsabili trattamento esterni Componenti organismi collegiali e commissioni istituzionali
TD02	Gestione del contenzioso e procedimenti disciplinari	Dirigente	Collaboratori del dirigente Responsabili trattamento esterni Segreteria Componenti organismi collegiali e commissioni istituzionali

TD03	Organismi collegiale e commissioni istituzionali	Dirigente Componenti organismi collegiali e commissioni istituzionali	Collaboratori del dirigente Collaboratori Scolastici Responsabili trattamento esterni Docenti Segreteria
TD04	Alunni nelle fasi propedeutiche all'avvio dell'anno scolastico	Dirigente Segreteria	Collaboratori del dirigente Collaboratori Scolastici Responsabili trattamento esterni Docenti Componenti organismi collegiali e commissioni istituzionali
TD05	Alunni nell'attività didattica e nella valutazione	Dirigente Docenti	Componenti organismi collegiali e commissioni istituzionali Collaboratori del dirigente Collaboratori Scolastici Responsabili trattamento esterni Segreteria
TD06	**Scuole non statali**	TRATTAMENTO AL MOMENTO NON EFFETTUATO	
TD07	Rapporti scuola-famiglie: gestione del contenzioso	Dirigente	Collaboratori del dirigente Responsabili trattamento esterni Segreteria Componenti organismi collegiali e commissioni istituzionali
TD08	Atti di gestione finanziaria, contabile, patrimoniale	Dirigente Segreteria	Collaboratori del dirigente Responsabili trattamento esterni Componenti organismi collegiali e commissioni istituzionali
TD09	Rapporti istituzionali con enti e privati	Dirigente Segreteria	Componenti organismi collegiali e commissioni istituzionali Collaboratori del dirigente Collaboratori Scolastici Responsabili trattamento esterni
TD10	Gestone adempimenti DL 81/2008	Dirigente Responsabile o incaricato gestione DL. 81/2008	Segreteria Componenti organismi collegiali e commissioni istituzionali Collaboratori del dirigente Responsabili trattamento esterni
TD11	Gestione sito WEB	Dirigente Responsabile o incaricato gestione del sito WEB	Segreteria Componenti organismi collegiali e commissioni istituzionali Collaboratori del dirigente Responsabili trattamento esterni
TD12	Gestione videoriprese	Dirigente	Collaboratori del dirigente Autorità Giudiziarie e di polizia
TD13	Gestione qualità	Dirigente Responsabil incaricati gestione qualità	Segreteria Componenti organismi collegiali e commissioni istituzionali Collaboratori del dirigente Responsabili trattamento esterni

2.1 Dati sensibili o giudiziari

Il Codice, prevede garanzie particolari per la categoria dei dati cosiddetti sensibili, ovvero i dati personali che riguardano profili particolarmente delicati della sfera privata delle persone (salute, vita sessuale, sfera religiosa, politica, sindacale e filosofica, origine razziale ed etnica).

L'utilizzazione di questi dati determina effetti rilevanti nei confronti degli interessati ed anche la direttiva comunitaria in materia (n. 95/46/CE) ne disciplina in maniera particolarmente rigorosa il trattamento. È previsto quindi, sia a livello comunitario che dal Codice italiano, solo un numero limitato di eccezioni tra cui figura, in particolare, l'ipotesi in cui sulla base della legge o di una decisione dell'Autorità garante sia riconosciuta l'esistenza di un interesse pubblico rilevante e siano previste opportune garanzie.

Per i soggetti pubblici è rimasta operante la possibilità di trattare i dati sensibili quando ciò sia previsto da una norma di legge che specifichi espressamente talune condizioni (rilevanti finalità di interesse pubblico perseguite; dati personali che possono essere utilizzati; operazioni di trattamento eseguibili).

Per i casi in cui manchi tale specifica base normativa, si è prevista la possibilità per i soggetti pubblici di chiedere al Garante di individuare transitoriamente le rilevanti finalità di interesse pubblico non previste espressamente da una legge, da un decreto legislativo o da un decreto -legge e che possono giustificare l'utilizzazione dei dati sensibili.

Tali principi sono stati ribaditi dal nuovo Codice, che stabilisce l'obbligo da parte dei soggetti pubblici avrebbero di adeguare i propri ordinamenti ed instaurare le procedure per individuare i tipi di dati sensibili e giudiziari le operazioni di trattamento strettamente pertinenti e necessarie in relazione alle finalità individuate dalla normativa o dai provvedimenti del Garante.

La pubblicità che per legge deve essere data a tali provvedimenti, secondo i vari ordinamenti, deve porre poi il cittadino in condizione di conoscere, con un apprezzabile grado di chiarezza, con quali modalità sono utilizzate tali informazioni (vedi allegato B).

La scuola predispone quindi annualmente una verifica per l'identificazione dei trattamenti di dati sensibili compiuti nell'ambito della propria attività istituzionale, specificando per ciascuno di essi le operazioni di trattamento necessarie per il perseguimento delle finalità di rilevante interesse pubblico individuate dal Codice e precedentemente dal D.Lgs. 135/99, dal Provvedimento del Garante per la protezione dei dati personali N. 1/P/2000, nonché da espresse disposizioni di legge o di regolamento, quando non siano specificati i tipi di dati trattati e i tipi di operazioni eseguibili.

Nell' allegato C sono riportati i casi previsti dalla normativa, relativi all'identificazione dei trattamenti di dati sensibili o giudiziari compiuti dalla scuola nell'ambito della propria attività istituzionale

3 Banche di dati

I trattamenti effettuati con l'ausilio di strumenti elettronici e cartacei si avvalgono delle banche dati riportate in allegato D

Senza preventiva autorizzazione del responsabile del trattamento, non è permesso realizzare nuove ed autonome banche dati con finalità diverse da quelle già previste

I documenti (o copia degli stessi) non possono, senza specifica autorizzazione, essere portati fuori dai luoghi di lavoro, salvo i casi di comunicazione dei dati a terzi preventivamente ed esplicitamente autorizzati dal Responsabile del trattamento.

4 Il sistema informatico

La struttura del sistema informativo è riportata in allegato E

5 Locali in cui sono custoditi i dati

L'elenco dei locali in cui sono custoditi i dati è riportato nell'allegato F.

6 Compiti e Responsabilità

6.1 Titolare del trattamento

Per tutti i trattamenti effettuati presso la scuola e per tutti i dati personali gestiti dalle proprie articolazioni organizzative (allegato A trattamenti) e delle banche dati ad esse afferenti, in conformità a quanto previsto dall'Art. 28 del Codice, il titolare del trattamento è la stessa Scuola denominata Istituto Superiore " V. Capirola" di Leno (COD. MEC. BSIS00900X), rappresentata dal Dirigente Scolastico.

Compiti del titolare sono quelli di assolvere l'obbligo di notificazione e di comunicazione al Garante, di adottare, per quanto di competenza, le misure necessarie a garantire la sicurezza dei dati personali, di impartire ai Responsabili le necessarie istruzioni per la corretta gestione e tutela dei dati personali, ivi compresa la salvaguardia della loro integrità e sicurezza e di verificare periodicamente l'osservanza dell'attività svolta dai Responsabili rispetto alle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati.

6.2 Responsabili del trattamento

I responsabili preposti al trattamento sono nominati, con atto scritto, dal titolare tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Per quanto riguarda l' Istituto Superiore " V. Capirola" di Leno , i responsabili sono individuati anche considerando i criteri di organizzazione dell'Amministrazione e di autonomia gestionale.

Nei casi in cui l' Istituto Superiore " V. Capirola" di Leno, mediante apposite convenzioni, affida il trattamento o parti del trattamento dei dati a soggetti esterni, nomina il soggetto esterno responsabile del medesimo trattamento. Le clausole relative alle modalità del trattamento e alle misure di sicurezza sono specificamente approvate per iscritto.

Conseguentemente a quanto previsto dal Codice all' art.29, è stato individuato come responsabile del trattamento dei dati :

- Il D.S.G.A. per le unità organizzative denominate: SEGRETERIA e COLLABORATORI SCOLASTICI

La figura professionale preposta alle unità organizzative citate è stata nominata Responsabile del Trattamento dei dati personali raccolti negli archivi di tipo cartaceo esistenti presso l'unità di competenza o presso gli archivi comuni nonché dei trattamenti afferenti i dati personali contenuti nelle banche dati elettroniche utilizzate dall' Istituto Superiore " V. Capirola" di Leno che contengono dati di competenza delle specifiche articolazioni organizzative.

6.2.1 Istruzioni impartite dal titolare ai responsabili del trattamento

1. Rispettare le misure minime di sicurezza previste dalla normativa vigente sulla tutela dei dati personali e disporre gli interventi necessari ad assicurare un livello minimo di protezione dei dati personali, sulla base delle specifiche indicazioni contenute nei regolamenti adottati da questo Istituto, al fine di:
    - ridurre al minimo il rischio di distruzione o perdita, anche accidentale, dei dati trattati;
    - evitare l'accesso non autorizzato ai dati trattati;
    - prevenire trattamenti non conformi alla legge.
2. Individuare e comunicare al Dirigente i nominativi oppure le categorie o specifici profili di operatori incaricati del trattamento dei dati.
3. Procedere – ove necessario – al rilascio ed alla revoca delle autorizzazioni previste dagli artt. 12, 13 e 14 del Disciplinare Tecnico in materia di misure minime di sicurezza contenuto all'Allegato B) del D.Lgs. 196/2003, e verificare che l'accesso ai dati da parte degli incaricati sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate.
4. In merito al mantenimento delle autorizzazioni di cui al precedente punto 3, verificare – almeno una volta all'anno – la sussistenza delle condizioni che hanno determinato la loro emissione e, in caso di difetto, di procedere alla loro revoca.
5. Comunicare tempestivamente all'Amministratore di Sistema ogni atto ed evento che comporti una disattivazione immediata o modifica dei profili e delle autorizzazioni di accesso alle banche dati e ai programmi applicativi, come ad esempio: dimissioni, assunzioni, trasferimenti da/verso altre Aree/Servizi, cessazione, sospensione o revoca di incarico, variazioni di ruolo/responsabilità, etc.
6. Fornire agli incaricati, per iscritto, le istruzioni per il corretto trattamento dei dati personali, eseguendo gli opportuni controlli.

7. Controllare la pertinenza, non eccedenza e completezza dei dati rispetto alle finalità dei trattamenti di propria competenza.
8. Stabilire le modalità di gestione e le forme di responsabilità relative a banche dati condivise da più unità organizzative, d'intesa con gli altri responsabili.
9. Informare prontamente il Titolare di ogni questione rilevante ai fini di legge.
10. Rispondere tempestivamente all'interessato che richieda di conoscere informazioni relative all'attività di trattamento, ai sensi dell'art. 7 del D.Lgs 196/2003 e successive modifiche ed integrazioni.
11. Rispondere ai reclami degli interessati.
12. Collaborare con il Garante per la protezione dei dati personali nel caso di richiesta di informazioni o di verifiche sui luoghi.

6.2.2 Trattamenti di dati affidati all'esterno

I trattamenti dati con aziende esterne riguardano:

1. manutentori sistema informatico fornito dalla Provincia: Provincia di Brescia
2. Consulente DL 81/2008 Sicurezza sui luoghi di lavoro
3. Medico competente

Agli enti, agli organismi, alle aziende, alle associazioni, alle strutture accreditate e agli altri soggetti esterni all' Istituto Superiore " V. Capirola" di Leno che svolgono parte di trattamenti a seguito di contratti o convenzioni, viene attribuita la qualità di Responsabile del trattamento ai sensi dell'art. 29 del decreto legislativo 196/2003 e dell'art. 19.7 del Disciplinare tecnico allegato al Codice.

A tali responsabili vengono prescritte le seguenti istruzioni:

6.2.3 Istruzioni impartite dal titolare ai responsabili esterni del trattamento

1. individuare gli incaricati del trattamento e impartire loro istruzioni scritte che garantiscano la liceità, la correttezza e la sicurezza del trattamento;
2. attuare, dove necessari, gli obblighi di informazione e acquisizione del consenso nei confronti degli interessati;
3. garantire all'interessato l'effettivo esercizio dei diritti previsti dall'art. 7 del decreto legislativo n.196/2003, in ordine all'accesso ai dati e a tutti i diritti di aggiornamento, rettificazione, cancellazione e di opposizione al trattamento;
4. adottare tutte le cautele e gli accorgimenti di natura tecnica e organizzativa previsti dal D.Lgs. 196/2003 per assicurare che i trattamenti effettuati avvengano nel pieno rispetto della vigente normativa in materia di privacy e di sicurezza.

Nell'ambito della formalizzazione del contratto di appalto o comunque al momento dell'instaurazione del rapporto di collaborazione, si inseriranno anche anche i seguenti punti:

1. **Durata del trattamento effettuato dalla Vostra Azienda**. La Vostra Azienda è autorizzata ad effettuare trattamenti di dati per conto dell' Istituto Superiore " V. Capirola" di Leno. fino al termine di decorrenza del rapporto contrattuale in atto.
2. **Finalità del trattamento effettuato dalla Vostra Azienda**. La Vostra Azienda tratterà i dati esclusivamente per le finalità individuate nel rapporto contrattuale.
3. **Obbligo alla riservatezza**. Con la presente, la Vostra Azienda si impegna a non divulgare, diffondere, trasmettere e comunicare i dati di cui l' Istituto Superiore " V. Capirola" di Leno. è titolare del trattamento, se non nelle misura e nelle forme necessarie ad adempiere i termini del rapporto contrattuale in atto.
4. **Titolarità dei dati**. I dati a Voi comunicati sono e rimarranno sempre e comunque di titolarità esclusiva dell' Istituto Superiore " V. Capirola" di Leno, e pertanto non potranno essere venduti o ceduti, in tutto o in parte, ad altri soggetti, nemmeno alla conclusione del rapporto contrattuale.
5. **Misure minime**. Con la presente la Vostra Azienda si impegna a mettere in atto e a verificare regolarmente l'efficacia di adeguate e preventive misure contro i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta, comprese le misure minime di sicurezza fisica, organizzativa e logica prescritte dal D.Lgs. 196/2003.
6. **Verifiche**. E' data facoltà al Titolare dell' Istituto Superiore " V. Capirola" di Leno di verificare che la vostra Azienda in relazione ai dati affidativi applichi correttamente le misure di sicurezza qui definite.
7. **Conclusione o revoca dell'incarico**. All'atto della conclusione o della revoca dell'incarico conferito dall' Istituto Superiore " V. Capirola" di Leno alla Vostra Azienda, o in qualsiasi momento Vi venga richiesto per soppravvenute necessità, Vi impegnate a riconsegnare tutti i dati trattati o comunque ricevuti, comprese tutte le copie di backup effettuate e tutta la documentazione cartacea. La Vostra Azienda si impegna altresì a cancellare fisicamente dai propri sistemi e dai propri archivi elettronici e cartacei tutti i dati la cui titolarità è del Istituto Superiore " V. Capirola" di Leno.

Quando trattasi di persona fisica, libero profesionista, consulente esperto ecc. all'interno del contratto individuale, o in allegato ad esso, vengono incluse le seguenti disposizioni:

Ai sensi dell'art. 13 del Decreto legislativo 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali, l'amministrazione scolastica fa presente che i dati richiesti al contraente sono indispensabili per stipula del presente contratto e saranno trattati solo a questi fini come previsto dall'informativa di cui il contraente ha presa visione.

Il contraente è responsabile del trattamento dei dati cui verrà a conoscenza nell'espletamento del suo lavoro ai sensi dell'art. 29 del Decreto legislativo 30 giugno 2003, n. 196 e in osservanza dell'art. 19.7 del Disciplinare tecnico allegato al Codice, si stabilisce quanto segue. I dati personali relativi al nostro

personale, ai nostri utenti, che in passato vi abbiamo comunicato , o che in futuro vi comunicheremo , o ai quali potrete avere accesso nell' ambito delle operazioni che di volta in volta vi affideremo potranno essere da voi utilizzati esclusivamente per operazioni funzionali allo svolgimento dei compiti affidativi. Per i compiti affidatevi si fa riferimento al contratto fra noi stipulato. Il contraente si impegna a non divulgare e diffondere, i dati di cui l'istituto è titolare del trattamento, la comunicazione ad altri soggetti è consentita solo nei termini previsti dalla legge e nelle misura e nelle forme indispensabili ad adempiere i termini del rapporto contrattuale in atto. Nessun altro trattamento potrà essere posto in essere da parte del contraente, il quale si impegna anche a. mettere in atto e a verificare regolarmente l'efficacia di adeguate e preventive misure contro i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato e di trattamento non consentito o non conforme alle finalità della raccolta, comprese le misure minime di sicurezza fisica, organizzativa e logica prescritte dal D.Lgs. 196/2003. Si ricorda inoltre che nessuno dei nostri dati potrà essere trattenuto o gestito dal contraente qualora si giunga ad una rescissione del contratto. Durante o al termine del contratto, tutti i dati non più necessari allo svolgimento delle mansioni affidatevi vanno restituiti o distrutti. E' data facoltà al Titolare dell'Istituto Superiore "V. Capirola" di Leno di verificare che in relazione ai dati affidativi si applichino correttamente le misure di sicurezza stabilite dal Codice sul trattamento dei dati personali.

6.3 Incaricati del trattamento

Il Codice sulla privacy (art. 30) impone al titolare o ai responsabili del trattamento di designare gli incaricati del trattamento e di fornire loro istruzioni scritte per la corretta gestione dei dati. Ciascun responsabile del trattamento dell' Istituto Superiore " V. Capirola" di Leno. provvede a nominare nell'ambito della propria ripartizione gli incaricati del trattamento, provvedendo loro una serie di istruzioni. La finalità di queste istruzioni scritte è quella di fornire le indicazioni per il trattamento dei dati e individuare gli specifici trattamenti che l'incaricato può legittimamente effettuare conformemente alle proprie mansioni.

Almeno una volta all'anno il responsabile deve verificare ed, eventualmente, aggiornare l'elenco degli incaricati e dei relativi ambiti di trattamento consentiti (punti 14-15 e 27 del disciplinare tecnico). Pertanto è utile indicare in modo non generico anche l'individuazione delle banche dati cui l'incaricato può accedere, la definizione delle finalità per le quali si effettuano i trattamenti e l'eventuale ambito di comunicazione e/o diffusione all'esterno.

Inoltre, in forza degli specifici obblighi in materia di sicurezza imposti dal Codice e dal disciplinare allegato al Codice, è necessario dettare anche prescrizioni puntuali sulle misure di sicurezza adottate a tutela dei dati: queste misure dovranno essere osservate da ogni singolo incaricato.

Dal punto di vista gestionale, per quanto riguarda i dati trattati con strumenti elettronici, i diversi incarichi si concretizzano in un sistema di autenticazione al sistema informatico che prevede diversi profili di autorizzazione (punti 12-13 e 14 del disciplinare tecnico).

6.3.1 Istruzioni impartite dal responsabile agli incaricati del trattamento

1. Il trattamento deve svolgersi in modo lecito e secondo correttezza: i dati personali devono essere raccolti, registrati e trattati esclusivamente per le finalità inerenti l'attività svolta da ciascuno, indicate nella lettera di nomina;
2. è compito di ciascun incaricato verificare l'esattezza ed il grado di aggiornamento dei dati trattati; che i dati personali siano pertinenti, completi e non eccedenti le finalità per le quali sono stati raccolti o successivamente trattati, secondo le indicazioni ricevute dal Titolare o dal Responsabile;
3. i dati devono essere conservati rispettando le misure di sicurezza previste dalla normativa vigente nonché quelle predisposte dall' Istituzione Scolastica garantendo la massima riservatezza in ogni operazione di trattamento e, in particolare, ciascun incaricato dovrà:
    - per le banche dati informatiche, utilizzare sempre il proprio codice di accesso personale, evitando di operare su terminali altrui e/o di lasciare aperto il sistema operativo con la propria password inserita in caso di allontanamento anche temporaneo dal posto di lavoro, al fine di evitare trattamenti non autorizzati e di consentire sempre l'individuazione dell'autore del trattamento;
    - conservare i supporti informatici e/o cartacei contenenti i dati personali in modo da evitare che detti documenti siano accessibili a persone non autorizzate al trattamento dei dati medesimi;
    - con specifico riferimento agli atti e documenti cartacei contenenti dati personali ed alle loro copie, riporre gli stessi al termine delle operazioni affidate nei luoghi ad accesso controllato appositamente predisposti;
    - le copie di dati personali su supporti rimovibili sono permesse solo se costituiscono operazione del trattamento approvata dal responsabile. In ogni caso tali supporti devono avere un'etichetta che li identifichi e non devono essere mai lasciati incustoditi;
    - in caso si constati o si sospetti un incidente di sicurezza deve essere data immediata comunicazione al Responsabile del trattamento;
4. ciascun incaricato dovrà segnalare al titolare o al responsabile eventuali circostanze che rendano necessario od opportuno l'aggiornamento delle predette misure di sicurezza al fine di ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alla finalità della raccolta;
5. gli ambiti di comunicazione dei dati sono quelli previsti dalle leggi e dal regolamento del M.P.I.
6. nessun dato potrà essere diffuso a terzi senza la preventiva specifica autorizzazione del Titolare o del Responsabile del trattamento;
7. la massima riservatezza sui dati personali dei quali si venga a conoscenza nello svolgimento dell'incarico deve essere mantenuta per tutta la durata del medesimo e anche successivamente al termine stesso;

6.4 Particolari incarichi

Incarichi particolari riguardano: l'Amministratore di Sistema e il Custode delle password.

La figura dell'"Amministratore di sistema", data la sua particolarità, è stata fin da subito prevista all'interno delle procedure dell'istituzione scolastica. Si è proceduto in fase di nomina alla valutazione delle caratteristiche soggettive, procedendo con designazioni individuali all'interno delle quali sono stati definiti gli ambiti di intervento e le responsabilità connesse.

Si ritiene dunque di proseguire con tale figura e se necessario di distribuire su più incaricati, i compiti e le incombenze procedurali resi obbligatori dalle misure minime di sicurezza previste dal Disciplinare Tecnico e dal provvedimento generale del 27 novembre 2008.

Per il ruolo ricoperto all'interno dell'organizzazione scolastica e per le competenze tecniche, a tali figure si richiede anche un supporto attivo nel coadiuvare il proprio responsabile e il titolare nell'individuazione di puntuali istruzioni operative attinenti all'applicazione delle misure di sicurezza per il trattamento dei dati personali compiute attraverso strumenti elettronici, a specificazione e chiarimento di quelle generali impartite dai singoli responsabili, nonché il coordinamento dei relativi adempimenti riguardanti le procedure di autenticazione e autorizzazione, assieme all'assistenza in questo campo ai responsabili e agli incaricati del trattamento.

Ai sensi dell'art 4.1 Valutazione delle caratteristiche soggettive, del provvedimento generale del garante del 27 novembre 2008, l'attribuzione delle funzioni di amministratore di sistema deve avvenire previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento ivi compreso il profilo relativo alla sicurezza.

Si è scelto quindi di individuare due tipologie di amministratore di sistema, una esterna e una interna.

Amministratore di sistema interno, operazioni di routine:

- gestione dei codici e delle password di accesso per la configurazione degli apparati attivi per la trasmissione dei dati sulla rete, dei codici e delle password di accesso per la configurazione del server e l'accesso alle funzioni sistemistiche di manutenzione degli stessi;
- è abilitato al rilascio dei codici e delle password da assegnarsi alle eventuali terze parti da abilitarsi al collegamento al sistema informatizzato della scuola dall'esterno (ad esempio, i fornitori di procedure informatiche ai fini di consentire l'erogazione dell'assistenza da remoto);
- è incaricato di mantenere aggiornata la documentazione tecnica relativa alla configurazione hardware e software della rete e degli strumenti di sicurezza;
- è incaricato di garantire l'effettuazione delle operazioni di salvataggio delle banche dati elettroniche, la non accessibilità di tali copie da parte di terzi non autorizzati, l'efficacia delle procedure di ripristino in caso di danneggiamento dei dati, la distruzione delle copie non più necessarie per le finalità di ripristino;
- è incaricato di effettuare la verifica del buon esito del Backup, e il salvataggio dei log di Backup;
- è incaricato di assegnare a ciascun incaricato del trattamento il profilo di utenza corrispondente alle sole funzionalità necessarie alla attività istituzionale svolta dal medesimo, concordata con il responsabile del singolo trattamento;

- è incaricato di vigilare, assieme ai responsabili, che i codici per l'identificazione non siano assegnati ad altri incaricati, neppure in tempi diversi;
- è incaricato di garantire la disattivazione delle credenziali di autenticazione non utilizzate da almeno sei mesi (esclude quelle preventivamente autorizzate per soli scopi di gestione tecnica) e, di concerto con i responsabili, di disattivare le credenziali di autenticazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
- è incaricato di garantire gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti.
- è incaricato di garantire l'efficienza e la disponibilità della rete, dei sistemi informativi e della piattaforma di autenticazione;
- è incaricato di svolgere controlli atti a rilevare eventuali accessi non autorizzati alla rete e ai sistemi;

Amministratore di sistema ai Backup delle banche dati della segreteria, **interno**, operazioni di routine:

- è incaricato di garantire l'effettuazione delle operazioni di salvataggio delle banche dati elettroniche, la non accessibilità di tali copie da parte di terzi non autorizzati, l'efficacia delle procedure di ripristino in caso di danneggiamento dei dati, la distruzione delle copie non più necessarie per le finalità di ripristino;
- è incaricato di effettuare la verifica del buon esito del Backup, e il salvataggio dei log di Backup

Amministratori di sistema esterni: possono essere più d'uno e sono individuati in base alle mansioni previste per il loro intervento. Gli ambiti di intervento sono definiti dal contratto o nella lettera di incarico.

L'amministratore di sistema esterno referente per la segreteria: dovrà svolgere oltre agli interventi di routine, (solo su richiesta e a supporto degli amministratori di sistema interni o in loro sostituzione), i seguenti compiti :

- è incaricato di verificare l'adozione delle misure minime di sicurezza con periodicità almeno annuale

Ai sensi dell'art 4.2 *Designazioni individuali* e ***4.3 Elenco degli amministratori di sistema*** del provvedimento generale del garante del 27 novembre 2008 gli amministratori di sistema individuati per l'anno 2010 sono:

1. Amministratore di sistema dotazioni informatiche della segreteria: Matteo Mutti, Vittorio Galelli, ErnestoTonni
2. Amministratori di sistema rete didattica: Matteo Mutti, Vittorio Galelli, ErnestoTonni
3. Amministratore di sistema esterno, verifiche misure minime di sicurezza:

La descrizione degli incarichi è riportata nella lettera di nomina.

Ai sensi dell' art. 4.4 Verifica delle attività, l'operato degli amministratori di sistema è oggetto, con cadenza almeno annuale, di un'attività di verifica da parte del titolare o del responsabili del trattamento, in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza rispetto ai trattamenti dei dati personali previste dalle norme vigenti.

Tale verifica si è svolta in fase di revisione del documento è ha dato esito positivo.

Ai sensi dell' art. 4.5 Registrazione degli accessi, si è adottato un sistema di registrazione degli accessi tramite la predisposizione di un registro cartaceo, dove vengono riportate le registrazioni degli interventi effettuati dagli amministratori di sistema, sulle banche dati dell'istituzione scolastica. I suddetti interventi comprendono i riferimenti temporali e la descrizione dell'evento che li ha generati e sono conservati per un congruo periodo, non inferiore a sei mesi.

Gli accessi alle banche dati avvengono di norma in presenza di una delle figure individuate come amministratore di sistema interno.

Si provvederà allo studio di sistemi di report automatico, (registrazione e conservazione) dei log di accesso degli amministratori di sistema.

Custode delle parola chiave è il soggetto preposto alla custodia delle parole chiave (utilizzate dagli incaricati per l'accesso ai dati e dall'Amministratore di Sistema) o che ha accesso alle informazioni che concernono le medesime; la figura del custode delle parole chiave è stata ampiamente rivalutata dal D.Lgs. 196/2003, che dedica a questa figura l'intero articolo 10 dell'Allegato B: "*quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante l'uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato, che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato*";

Il Custode delle Parole Chiave deve attenersi scrupolosamente alle seguenti istruzioni:

1. Richiedere ed ottenere con cadenza almeno trimestrale da ogni incaricato del trattamento una busta chiusa e sigillata datata e firmata all'esterno, contenente l'elenco di tutte le credenziali di accesso alle banche dati dell'istituzione scolastica;
2. richiedere e ottenere, con cadenza almeno semestrale, dagli Amministratori di Sistema, una busta chiusa e sigillata, datata e firmata sul lato esterno, contenente l'elenco dei codici identificativi personali e delle corrispondenti parole chiave, relative ai profili per la gestione del sistema utilizzati per l'accesso a livello di rete; questo elenco dovrà comprendere inoltre anche i codici identificativi personali e le parole chiave relative ai router, ai firewall, agli switch, e in generale a tutti gli apparati di sicurezza e di connettività gestiti dalla scuola,
3. depositare le suddette buste in un armadio con serratura o ulteriore contenitore più sicuro,

4. a campione, e con una certa frequenza, aprire il contenuto delle buste ottenute e verificare che le password contenute siano effettivamente quelle in uso; dopo aver effettuato il controllo, darne notifica al titolare del trattamento e agli incaricati oggetto dell'ispezione che provvederanno alla modifica della password sottoposta a verifica
5. in caso di comprovata necessità, dovrà recuperare le buste contenenti le parole chiave di sistema e utilizzare le parole chiave per assicurare la disponibilità dei dati e delle applicazioni, dandone contestuale notifica al Titolare del trattamento dei dati e all'incaricato del trattamento

Per questioni di funzionalità sarebbe meglio prevedere più di un custode delle password.

6.5 Figure definite dall' Istituto Superiore "V. Capirola" di Leno, nella stesura del presente DPS

In questo paragrafo sono evidenziate le figure formalmente definite dal Istituto Superiore " V. Capirola" di Leno, prima della revisione del presente DPS. Di seguito si riportano gli abbinamenti tra le figure previste dalla legge e quelle formalmente definite dalla scuola.

Figura prevista dalla legge	**Figura definita**	**Note**
Titolare del trattamento dei dati	Individuata ipso jure nel Istituto Superiore " V. Capirola" di Leno inteso come persona giuridica, legalmente rappresentato dal Dirigente Scolastico	Nel caso di una Pubblica Amministrazione il Titolare è l'entità nel suo complesso, intesa come persona giuridica (Art. 28 D.Lgs. 196/2003).
Responsabile del trattamento dei dati	DSGA	I compiti e istruzioni assegnate per iscritto
Incaricato del trattamento dei dati	Figure individuate	I compiti e istruzioni assegnate per iscritto
Amministratore di Sistema interni	Figura individuata	Si occupa dei bk, upgrade, password, ne sono stati individuati 4
Amministratore di Sistema esterno	Figura da individuare	Fornisce supporto tecnico agli amministratori interni e li sostituisce quando necessario, gestisce specifiche banche dati
Custode delle parole chiave	Figure individuate	
Aziende esterne coinvolte nel processo di trattamento dei dati	Nomine effettuate	Incluse specifiche nei contratti

7 Misure di sicurezza

7.1 Misure di sicurezza adottate

L'obiettivo principale del presente capitolo è documentare le misure di sicurezza individuate ed implementate precedentemente all'analisi dei rischi ed a valle dell'analisi e della quantificazione dei rischi effettuata nel capitolo precedente.

Le misure di sicurezza individuate sono di varia natura, a seconda dell'ambito di applicazione, della modalità di messa in opera e della tipologia di soggetti che sono tenuti a rispettarle.

7.1.1 Misure organizzative

Sono stati analizzati i trattamenti in atto e definiti in dettaglio i ruoli e le responsabilità relative al trattamento dei dati, procedendo alla nomina di un responsabile del trattamento, corredata da dettagliate istruzioni.

Il responsabile ha a sua volta proceduto alla designazione degli incaricati del trattamento, a cui sono state fornite dettagliate istruzioni scritte. Contestualmente sono stati nominati anche un amministratore di sistema, un incaricato del BK e un custode delle credenziali, ai quali sono affidati incarichi specifici.

In allegato alle nomine di Incaricato sono state forniteanche istruzioni per un corretto e sicuro utilizzo dei sistemi informativi scolastici.

7.1.2 Misure per la sicurezza fisica e ambientale

L' Istituto Superiore " V. Capirola" di Leno ha implementato tutte le misure di sicurezza previste dalla normativa vigente, le nomine dei RSPP, RSL, medico competente e il consulente per il DL. 81/2008 sono agli atti della scuola.

Per quanto riguarda le misure di protezione dagli incendi e la sicurezza sui luoghi di lavoro si fa riferimento alla documentazione prevista dal DL. 81/2008 e successive, agli atti della scuola, unitamente al piano di emergenza antincendio.

7.1.3 Protezione delle aree e dei locali

Di seguito sono sinteticamente riportati i criteri tecnici ed organizzativi per la protezione delle aree e dei locali interessati alle misure di sicurezza nonché le procedure per controllare l'accesso delle persone autorizzate ai locali medesimi.

Ulteriori informazioni sulle misure di sicurezza previste in questo settore sono riportate nell'allegato F descrizione locali in cui sono custoditi i dati.

7.1.4 Controllo accesso ai locali

Gli stabili dove sono conservati e trattati i dati dispongono di un accesso controllato a vista durante l'orario lavorativo. Nella varie sedi la sorveglianza è garantita dal personale ausiliario nelle ore diurne ed è protetta da un sistema di antifurto in quelle notturne (vedi allegato F).

7.1.5 Autorizzazioni all'ingresso nei locali

Le autorizzazioni all'ingresso nei locali vengono concesse sulla base dei compiti assegnati dal piano di lavoro discusso ad inizio d'anno, ogni mutamento o accesso diversificato avviene previa autorizzazione del Dirigente o del DSGA.

7.2 Protezione dell'integrità e della disponibilità dei dati

7.2.1 Hardware

Tutte le strutture hardware (dispositivi di connessione, serve, client, altri dispositivi) sono scelti in base a caratteristiche di affidabilità e sono periodicamente controllati.
Non è consentita agli utenti l'installazione o l'uso di alcun dispositivo di memorizzazione, comunicazione o altro se non con l'autorizzazione esplicita dell'Amministratore di sistema
L'alimentazione del server è garantita da un gruppo di continuità in grado di fornire l' energia elettrica sufficiente ad effettuare, se necessario, le operazioni di spegnimento senza pregiudicare l'integrità dei dati.

7.2.2 Software

Gli strumenti software utilizzati sono adottati solo dopo attenta valutazione e comunque con l'approvazione dell'Amministratore di sistema. Elenco del Software utilizzato è riportato nell'allegato G.
Non è consentito l'uso di programmi diversi da quelli distribuiti ufficialmente dalla scuola (dlg. 518/92 sulla tutela giuridica del software e L. 248/2000 nuove norme di tutela del diritto d'autore) su indicazione dell'Amministratore di sistema.
Gli incaricati del trattamento sono stati informati sulle correte modalità di trattamento, sulle procedure per garantire il salvataggio dei dati e sui pericoli per la sicurezza.
L'utilizzo ordinario degli strumenti elettronici relativo al database SISSI è compiuto da personale con privilegi "user", che non permettono di compiere operazioni che mettano in pericolo il software utilizzato per la gestione dei dati.
Il personale che deve operare con diritti di amministratore dispone di una documentazione adeguata e può avvalersi della consulenza di idonee e qualificate persone esterne.

7.2.3 Procedure di salvataggio e ripristino dei dati

Per ogni archivio permanente viene tenuta una copia di back up e sono effettuate registrazioni su supporti differenti in modo da poter permettere la ricostruzione dei dati a fronte di cancellazioni o danneggiamenti.

Il sistema di Backup in merito ai database di sissi, argo e dei dati salvati sul database tabelle viene effettuato su un server esterno.

La cartella Dropbox inserita su tutti e 2 i server (su server01 in E:\Dropbox, su server03 in X:\Dropbox).
All'interno si trovano 3 cartelle:Argo,Sissi e SQL

I backup dei database si salvano automaticamente la domenica notte nelle rispettive cartelle. La stessa struttura di directory (partendo dalla cartella Dropbox) è sincronizzata sui 2 server e nell'area riservata e criptata in internet.

L'amministratore di sistema, e l'eventuale responsabile del Bk, verifica periodicamente il file di log fornito dal sistema di Bk per rilevare eventuali problemi, questo file di log viene conservato per eventuali controlli almeno per 1 anno. La prova di ripristino effettuata ha dato esito positivo, l'amministratore di sistema provvederà periodicamente ad effettuarne altre.

Di ogni documento elettronico viene effettuata copia cartacea.

Ripristino intero sistema: in caso di necessità di ripristino a seguito di guasto viene coinvolto il fornitore dei servizi di assistenza hardware e software. Il fermo macchina è in funzione del tipo di guasto verificatosi. In caso di previsione di tempi superiori ai 7 giorni verranno adottate soluzioni temporanee per garantire la ripresa, anche parziale, della disponibilità dei dati su sistemi alternativi.
Il contratto di assistenza stipulato con il fornitore prevede il ripristino del guasto entro 5 giorni lavorativi.
Viene inoltre programmata una manutenzione preventiva almeno ogni 6 mesi dove sono previsti i seguenti interventi: controllo aggiornamenti automatici delle vulnerabilità, controllo efficacia antivirus, controllo efficacia sistema di Bk e prove di ripristino dati, verifica installazione mailware.

7.2.4 Custodia supporti informatici di backup

I supporti informatici di backup sono custoditi in un armadio di una stanza chiusa a chiave.

7.2.5 Protezione da virus e programmi pericolosi

Per la prevenzione di tali rischi sono in vigore misure tecniche ed organizzative.

Tra le misure di sicurezza tecniche si inserisce l'installazione diffusa e controllata di software antivirus. Tali programmi sono installati in tutte le stazioni di lavoro in cui vengono svolti trattamenti in rete e a protezione di tutti i server di rete.

Il software adottato è: CA Security Center sui server e Avir sui client, entrambi permettono una gestione attiva della protezione antivirus e l'aggiornamento continuo delle regole di protezione.
Il modulo antivirus sempre attivo in memoria intercetta tutte le operazioni eseguite dall'utente eseguendo una scansione da virus ogni volta che un file viene aperto, copiato, creato e rinominato oltre ai controlli sui floppy disk inseriti anche all'accensione e allo spegnimento del computer. Ciò permette di isolare i virus riconosciuti prima che possano diffondersi. Il programma antivirus permette anche controlli a richiesta, periodicamente o quando necessario vengono eseguite scansioni dai virus conosciuti su tutti i programmi e documenti presenti sul personal computer al fine di permettere la eventuale pulizia dei virus penetrati.
A protezione dai virus sono state emanate norme di comportamento interne e note informative, riassunte nelle istruzioni fornite agli incaricati, assieme al divieto di utilizzare software non ufficialmente autorizzato dalla scuola e preventivamente testato nella sua integrità. Tale norma assicura anche il rispetto dei contenuti del dlg. 518/1992 e modificazioni successive sul diritto d'autore e la tutela legale del software.

7.2.6 Prevenzione dalle vulnerabilità e aggiornamento dei sistemi

Sono in atto procedure automatiche e manuali per l'aggiornamento dei sistemi e la prevenzione delle vulnerabilità.
L'attuazione e il controllo delle procedure sono affidate agli Amministratori di sistema, che si avvalgono per lo svolgimento dei loro compiti, anche dei resp. del BK e se necessario si avvarranno di un consulente esterno.

7.3 Protezione della riservatezza dei dati

7.3.1 Protezione della rete

La rete di istituto è basata sulle seguenti apparecchiature attiveHP Procurve 5304 XL 2600 e 1800 queste permettono la sua suddivisione in tante VLAN fraloro separate e protette.

vlan 1
Rete di servizio per gli apparati attivi di rete

vlan 11, vlan 12, vlan 21, vlan 22, vlan 31, vlan 32, vlan 33, vlan 34, vlan 35, vlan 41, vlan 42, vlan 43, vlan 44, vlan 45, vlan 46, vlan 47, vlan 48
Reti dei laboratori

vlan 5
Rete di servizio per il collegamento ad internet (collega il punto di arrivo dell'adsl al ced)

vlan 7
Rete per l'accesso all'escuola fornito dalla Provincia di Brescia

vlan 4
Rete per i server e per gli uffici

vlan 101
Rete didattica

Restrizioni
La vlan7 consente l'accesso solo al portale dell'escuola
Le vlan dei laboratori consentono l'accesso solo al server nominato server03 che gestisce il dominio Alunni, e al server proxy

Per la protezione dei dati presenti sulla Lan dai pericoli provenienti dall'esterno della rete e in particolare da Internet, è in funzione il seguente Firewall iptables installato sul proxy.

Il sistema di sicurezza da e verso internet è composto dai seguenti moduli:
squid: web proxy (utilizzato da docenti e alunni)
iptables: firewall
apache: web server per l'intranet della scuola
openvpn: gestisce la vpn tra le 2 sedi Leno e Ghedi

Per i laboratori Autocad e internet è attivo il sistema Key Student conforme alla direttiva europea 95/4 decreto Pisanu.

7.3.2 Sistema di autenticazione

L'autenticazione di tutti i client della rete avviene su un dominio con Active Directiory Windows 2003 Server per la retre didattica e windows 2000 server per la segreteria.

Il sistema utilizzato consente all'utente di accedere ai computer con un'identità che può essere autenticata e autorizzata all'accesso alle risorse di locali e di rete. Ciascun utente che accede alla rete dispone di un account utente e di una password univoci.
L'autenticazione avviene mediante l'inserimento delle credenziali personali dell'utente: codice utente e parola chiave (componente riservata nota solo all'utente).
Ogni utente è in grado di modificarsi la password e comunque ogni 90 giorni il sistema obbliga tutti a tale modifica, diversamente passato tale termine l'utente viene disabilitato. I criteri di composizione della password prevedono una lunghezza minima di 8 caratteri, la presenza di numeri e lettere maiuscole e minuscole. Non è possibile ripetere la stessa password.
Dopo cinque accessi con password errata il sistema disabilità l'account.
L'accesso al gestionale SISSI è consentito solo agli utenti autorizzati e nell'ambito di specifici profili che prevedono permessi e privilegi differenziati a seconda delle principali mansioni svolte. L'accesso viene effettuato con userid univoca e con password di minimo 8 caratteri e (lettere e numeri), per il gestionale SISSI e gli accessi alla WEB INTRANET e al nuovo sistema telematico SIDI ogni utente è in grado di cambiarsi la password di accesso. Per quanto riguarda l'accesso a SIWEB che sarà progressivamente sostituito dal SIDI le credenziali e i privilegi di accesso di quest'ultimo, sono fornite dal MIUR e sono gestibili dal Dirigente o dal DSGA. La gestione dei servizi telematici quali Entratel, INPS, INPDAP ecc sono fornite dai gestori del servizio, si veda allegato G.

Descrizione delle modalità di accesso e del software per la didattica.

Gli utenti (amministrativi, docenti) accedono agli applicativi del programma dal PC in seguito al proprio account di rete (primo livello di protezione). Il programma "M.A.R.T.I.N.A.", ricavato dai moduli GEMMA del prof. Scolari ma rivisto e ampliato nelle funzionalità è costituito da una parte back-office (tabelle dei dati su server MS SQL) e una serie di applicazioni front-office (per ora basate su MS Access sia come maschere che come report) collegate al DB SQL e diversificate a seconda delle funzioni richieste e degli utenti (es. Anagrafica alunni per la segreteria Alunni, ScrutiniProfe per l'inserimento delle valutazioni e la conduzione degli scrutini nella parte a loro riservata da parte dei soli docenti). Solo chi fa parte di uno di questi gruppi (Docenti, Amministrativi) può eseguire questi applicativi (permessi assegnati con l'Active Directory). Inoltre una volta avviato il programma, vi è la richiesta di una ulteriore password breve generata in modo casuale all'inizio delle procedure e assegnata al docente da parte della segreteria. Questa password permette al docente di inserire i voti relativi alle sole proprie classi e di controllarne la situazione generale. La segreteria al termine dello scrutinio ha la facoltà e l'obbligo di "bloccare la classe" per impedire ulteriori variazioni. La stessa ha inoltre delle funzioni più ampie per poter svolgere le altre funzioni (stampe certificati, pagelle, situazione debiti, ecc.)

7.3.3 Sistema di autorizzazione

Una volta autenticati, gli utenti hanno accesso solo ai dati e alle applicazioni per le quali sono incaricati del trattamento. Per l'archiviazione dei documenti generici sul server, gli ciascun gruppo omogeneo di incaricati dispone di una propria cartella.

8 Analisi dei rischi che incombono sui dati

L'analisi dei rischi è stata condotta secondo le dimensioni di analisi previste dalla normativa vigente e dalla conoscenza del contesto specifico. Una approccio globale alla sicurezza richiede però di considerare globalmente gli aspetti ambientali (sicurezza fisica), tecnici (sicurezza fisica e logica), organizzativi (definizione di ruoli, procedure, formazione) ed infine legali (leggi e raccomandazioni, normative). L'analisi dei rischi è stata quindi condotta analizzando anche aspetti tecnici e organizzativi più ampi rispetto alle prescrizioni legislative.

L'analisi è stata focalizzata in particolare sulle circostanze possibili o probabili che possano costituire il verificarsi di rischi di distruzione o perdita, anche accidentale, dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta.

Tutti i rischi esaminati sono stati individuati, classificati e descritti nei seguenti principali raggruppamenti:

- rischi organizzativi e legali;
- rischi per l'integrità o la disponibilità dei dati;
- rischi per la riservatezza dei dati;

8.1 Rischi organizzativi e legali

I rischi analizzati in questa sezione sono legati prevalentemente a possibili errori o omissioni rispetto agli adempimenti previsti dalla normativa che possono comportare casi di trattamento non consentito o non conforme alle finalità della raccolta.

L'importanza di queste verifiche è sottolineata dal fatto che molti dei requisiti richiesti dalla normativa comportano, se non soddisfatti, il pericolo di pesante sanzioni, penali ed amministrative.

Codice rischio	Elemento di rischio	Livello di rischio	Note
RO-01	Trattamento di dati non corretto o non lecito in violazione art.18-19.	Basso	L' Istituto Superiore " V. Capirola" di Leno. effettua trattamenti di dati personali solo nell'ambito dello svolgimento delle proprie funzioni istituzionali, osservando i presupposti e i limiti stabiliti dal presente codice.
RO-02	Trattamento in violazione alle prescrizioni sui dati sensibili e giudiziari (art.20-21-22).	Basso	Sono state disposte opportune istruzioni per l'individuazione dei dati sensibile e giudiziari e il loro conseguente trattamento. Si è recepito e applicato l'apposito regolamento emanato dal Ministero della Pubblica Istruzione

RO-03	Omessa o inidonea informativa all'interessato in violazione alle prescrizioni dell'art. 13.	Basso	Sono state predisposte le idonee informative all'interessato.
RO-04	Trattamento in violazione alle prescrizioni dell'art. 29 (individuazione, nomina, compiti e istruzioni per i responsabili).	Basso	Si è provveduto alla nomina dei Responsabili del Trattamento
RO-05	Trattamento in violazione alle prescrizioni dell'art. 30 (individuazione, nomina, compiti e istruzioni per gli incaricati).	Basso	Sono stati nominati incaricati del trattamento e a fornite loro adeguate istruzioni.
RO-06	Trattamento in violazione alle prescrizioni dell'art. 34 (misure di sicurezza per i trattamenti con strumenti elettronici).	Basso	Sono state implementate le misure di sicurezza previste dal codice.
RO-07	Trattamento in violazione alle prescrizioni dell'art. 35 (misure di sicurezza per i trattamenti senza strumenti elettronici).	Basso	Gli archivi presso la sede sono chiusi e hanno accessi controllati.
RO-08	Trattamento in violazione alle prescrizioni sui divieti di trasferimento dei dati all'estero (art.42-43-44-45).	Basso	I trasferimenti riguardano esclusivamente dati comuni necessari all'adempimento di eventuali scambi culturali deliberati dagli Organi Collegiali, previo il consenso dei genitori degli alunni partecipanti.
RO-9	Trattamento in violazione alle prescrizioni sulla videosorveglianza (art. 134).	Basso	I dati rilevati tramite apparati di videosorveglianza o registrazione di immagini sono trattati in conformità al codice
RO-10	Mancata individuazione dei criteri da adottare nel caso di affidamento dei dati all'esterno della struttura del titolare.	Basso	I dati affidati all'esterno sono regolati da una convenzione sotto l'aspetto della loro sicurezza.
RO-11	Assenza o inadeguatezza di un programma di formazione e sensibilizzazione degli incaricati sulle problematiche della sicurezza e della privacy.	Basso	Il personale ha partecipato alle riunioni informative. Per tutti è stato messo a dsisposizione il cd fornito dal MIUR.

Il Codice prevede in sostanza tre ordini di sanzioni:

- quelle di *carattere amministrativo*, disciplinate dagli articoli da 161 a 166;
- quelle di *natura penale*, disciplinate dagli articoli da 167 a 172;
- le sanzioni *indirette*, che conseguono dai provvedimenti del Garante.

Queste ultime, pur non essendo classificabili tra le sanzioni in senso proprio, consistono nella facoltà del Garante di vietare, in tutto o in parte, il trattamento dei dati o di disporne il blocco quando, in considerazione della natura dei dati, delle modalità del trattamento o degli effetti che esso può determinare, vi è il concreto rischio del verificarsi di un pregiudizio rilevante, per uno o più interessati.

Anche quest'ultimo ordine di sanzioni, che è stato oggetto di commento in precedenza, merita la massima attenzione, perché è lampante che, in molti casi, l'adozione di questi provvedimenti potrebbe avere effetti dirompenti sulla attività del soggetto che tratta i dati, sino a paralizzare di fatto la sua attività.

(i) Legge n. 547/1993 - Crimini informatici commessi da dipendenti ed addebitabili all'azienda

Inoltre, la legge 547/93 ha introdotto nel nostro ordinamento vari "crimini informatici", ovvero l'attentato a impianti informatici di pubblica utilità, falsificazione di documenti informatici, accesso abusivo ad un sistema informatico o telematico, detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici, diffusione di programmi diretti a danneggiare o interrompere un sistema informatico, violazione di corrispondenza telematica, intercettazione di e-mail, danneggiamento di sistemi informatici o telematici (...).

Il datore di lavoro rischia di essere ritenuto in concorso con il dipendente a lui subordinato che ha commesso il crimine informatico, per non aver posto in essere tutte le misure di prevenzione e controllo idonee a garantire la sicurezza del trattamento dei dati.

La mancata adozione di tutte le misure idonee a ridurre al minimo i rischi viene considerata difatti un agevolazione alla commissione del crimine.

8.2 Rischi per l'integrità e la disponibilità dei dati

L'accertamento dell'integrità dei dati ha riguardato la protezione dei dati stessi dai rischi di possibili modifiche o distruzione, accidentali o deliberate, classificati in:

1) rischi ambientali,
2) rischi specifici per trattamenti con strumenti elettronici,
3) rischi specifici per trattamenti senza l'ausilio di strumenti elettronici.

8.2.1 Rischi ambientali

I rischi ambientali costituiscono la componente più classica dei rischi, quella che riguarda la sicurezza dei locali e degli strumenti che ospitano i dati. Di questa tipologia fanno parte eventi naturali come terremoti, allagamenti e frane ed eventi dolosi come l'incendio, l'intrusione, gli atti di vandalismo e il furto.

In particolare per i possibili disastri naturali si è tenuto conto della zona in cui sorgono facendo riferimento al documento di prevenzione dei rischi adottato dall'istituto ai sensi della legge 626.

Si è tenuto conto poi della frequenza di altri eventi calamitosi (es. frane), la vicinanza di importanti vie d'acqua che potrebbero esondare.

8.2.2 Rischi specifici per trattamenti con strumenti elettronici

L'accertamento dell'integrità e della disponibilità dei dati ha riguardato la protezione dei dati stessi dai rischi di possibili modifiche o distruzione accidentali o deliberate o il fatto che le informazioni non siano disponibili a causa di eventi come:

- Sovrascrittura o distruzione dei dati, involontarie ma imputabili ad azioni umane errate;
- Sovrascrittura o distruzione dei dati dovute a guasti delle apparecchiature dedicate alla memorizzazione;
- Alterazioni dei dati conseguenti ad una teorica azione deliberatamente perpetrata allo scopo di modificare volontariamente i dati, inserire nuovi dati o distruggere i dati;
- Alterazioni, distruzione o indisponibilità dei dati connessi alla diffusione dei virus e dei programmi pericolosi, provocata da corruzione dei file eseguibili, corruzione dei dati stessi; corruzione di documenti; perdita di file; perdita di spazio utilizzabile nelle memorie; cattivi funzionamenti del sistema; degrado delle prestazioni del sistema; impossibilità di utilizzo del sistema;
- Distruzione o alterazione dei dati dovuta a deterioramento nel tempo dei supporti di memorizzazione e del mezzo fisico che li ospita;
- Danneggiamento o manomissione delle attrezzature e/o delle connessioni;
- Indisponibilità dei dati dovuta ad anomalie in programmi che avrebbero dovuto elaborare i dati e che non hanno potuto completare la loro esecuzione ("abend" di procedure per input errati, o errori di realizzazione);
- Indisponibilità dei dati malfunzionamento hardware (guasti alle unità di elaborazione, di memorizzazione o di trasmissione);
- Indisponibilità dei dati per dimensionamento non sufficiente delle risorse tecnologiche deputate alla trasmissione ed alla memorizzazione.

8.2.3 Rischi specifici per trattamenti senza l'ausilio di strumenti elettronici

- Furto, danneggiamento o distruzione dei supporti cartacei sui quali sono conservati i dati;
- Mancanza di procedure adeguate di archiviazione che consentano la disponibilità e la reperibilità dei dati.

Codice rischio	Elemento di rischio	Livello di rischio	Note
Rischi ambientali			
RI-01	Allagamento	Basso	Non si rilevano particolari pericoli di allagamento.
RI-02	Rischio sismico	Basso	Vedere piano emergenza e documentazioni DL. 81/2008 agli atti della scuola
RI-03	Altre calamità naturali	Basso	idem
RI-04	Incendio	Basso	idem
Rischi specifici per i trattamenti con strumenti elettronici			
RI-05	Danneggiamento o perdita di dati dovuto a discontinuità nell'alimentazione elettrica.	Basso	A protezione del server è in uso un gruppo di continuità adeguato alle esigenze minime
RI-06	Danneggiamento o perdita di dati dovuto a malfunzionamenti hardware.	Basso	Le caratteristiche delle risorse hardware preposte al trattamento dei dati risultano adeguate alle esigenze.
RI-07	Presenza di anomalie e difetti software che minacciano l'integrità dei dati.	Basso	I software applicativi utilizzati non presentano anomalie .
RI-08	Danneggiamento o perdita di dati dovuto all'azione di programmi di cui all'art.615 quinquies del c.p.(Virus, Spamming e simili)	Basso	Aggiornamento automatico giornaliero dell'antivirus, impartite idonee istruzioni agli operatori.
RI-09	Danneggiamento o perdita di dati dovuto alle vulnerabilità di sistemi operativi e software applicativi.	Basso	Sono in atto procedure di correzione delle vulnerabilità.
RI-10	Danneggiamento o perdita di dati dovuto a deterioramento nel tempo dei supporti di memorizzazione.	Basso	Sono in atto regole per i supporti di memorizzazione.
RI-11	Possibilità di asportare o manomettere le unità disco.	Basso	Non si riscontrano particolari pericoli di asportazione o manomissione
RI-12	Possibilità di furto delle risorse hardware.	Basso	E' presente un sistema di antifurto,
RI-13	Cancellazione o modifica non autorizzata dei dati.	Basso	Le procedure in atto, non prefigurano particolari rischi .
RI-14	Assenza o inefficienza di sistemi di backup.	Basso	Sono in atto procedure adeguate di backup.
RI-15	Incapacità o difficoltà a ripristinare copie di backup.	Basso	Sono state effettuate prove di ripristino, con esito positivo
Rischi specifici per trattamenti senza l'ausilio di strumenti elettronici			
RI-16	Rischio di furto, danneggiamento o distruzione dei dati in forma cartacea.	Basso	E' presente un sistema di antifurto,

8.3 Rischi per la riservatezza dei dati

Per quanto attiene la "riservatezza" si è fatto riferimento alla natura ed al grado di confidenzialità, riservatezza e particolarità dei dati, al fine di garantire la dovuta necessaria riservatezza delle informazioni proteggendole da ipotetiche divulgazioni non autorizzate, consentendone l'utilizzo ed il trattamento solamente ai soggetti fisici incaricati dei trattamenti.

Tale rischio è stato esaminato in relazione alla possibilità che si realizzino rilasci di informazioni non autorizzate e/o accessi non autorizzati ai dati.

Gli eventi controllati posti in relazione al rischio di accessi non autorizzati è stato determinato sulla base delle seguenti due fattispecie:

1. Rischi specifici per trattamenti con l'ausilio di strumenti elettronici;
2. Rischi specifici per trattamenti senza l'ausilio di strumenti elettronici.

8.3.1 Rischi specifici per trattamenti con l'ausilio di strumenti elettronici

1. Dovuti ad un "profilo" di autorizzazione all'accesso non aderente al ruolo assegnato o conseguente all'attribuzione di "privilegi" di accesso eccessivi.
2. Dovuti ad "impersonificazione" di un dipendente autorizzato all'accesso ai sistemi.
3. Dovuti ad accessi tramite sistemi di collegamento remoto installati per la manutenzione o la trasmissione di software.
4. Dovuti ad intercettazione di comunicazioni telematiche.
5. Dovuti alla possibilità di intrusioni ed accessi non autorizzati all'interno della rete locale e dei server

8.3.2 Rischi specifici per trattamenti senza l'ausilio di strumenti elettronici

1. Dovuti ad una mancata informazione e sensibilizzazione sulle regole di custodia da parte degli incaricati.
2. Dovuti a una scarsa protezione degli archivi.
3. Dovuti a mancata suddivisione dei dati più sensibili dai dati comuni.

Codice rischio	Elemento di rischio	Livello di rischio	Note
Rischi di accesso non autorizzato ai dati trattati con strumenti elettronici			
RR-01	Sistema di autenticazione mancante, non adeguato o non utilizzato correttamente.	Basso	Il sistema di autenticazione è adeguato
RR-02	Rischio di perdita di riservatezza delle credenziali di autenticazione dovuto a mancata custodia della password.	Basso	Sono state fornite istruzioni sulla custodia delle password.
RR-03	Rischio di perdita di riservatezza delle credenziali di autenticazione dovuto a password deboli o facilmente decodificabili.	Basso	E' in atto una politica di controllo della robustezza delle password.
RR-04	Profili di autorizzazione mancanti o non definiti correttamente.	Basso	Sono in atto procedure di verifica dei profili di autorizzazione
RR-05	Rischi legati ad accessi tramite sistemi di collegamento remoto installati per la manutenzione o la trasmissione di software.	Basso	Sistema non attivato sui PC. VPN attiva e protetta fra server sedi Leno e Ghedi
RR-06	Rischi legati ad intercettazione di comunicazioni telematiche.	Basso	A protezione della linea WAN è installato un firewall
RR-07	Possibilità di intrusioni ed accessi non autorizzati all'interno della rete locale e dei server, dovuti a mancanza di protezione perimetrale.	Basso	IDEM
RR-08	Possibilità di intrusioni ed accessi non autorizzati all'interno della rete locale e dei server, dovuti a scarsa efficacia della protezione fornita dal firewall.	Basso	IDEM
RR-09	Possibilità di diffusione di dati a causa di programmi di cui all'art. 615-quinquies del C.P (virus e simili).	Basso	Modalità di aggiornamento dell' antivirus automatiche e impartite idonee istruzioni agli operatori
RR-10	Furto di supporti di memorizzazione	Basso	Non si evidenziano particolari rischi in tal senso.
RR-11	Furto di supporti di backup	Basso	I supporti sono custoditi in un armadio chiuso a chiave.
RR-12	Pubblicazione di dati su web server non protetti	Basso	Sono state fornite idonee istruzioni ai responsabili della gestione del sito WEB

Rischi di accesso non autorizzato ai dati trattati senza l'ausilio di strumenti elettronici			
RR-13	Mancata custodia da parte degli incaricati	Basso	Gli incaricati sono a conoscenza delle modalità corrette di custodia dei dati.
RR-14	Accesso non autorizzato a locali contenenti dati sensibili	Basso	L'accesso agli archivi è controllato.
RR-15	I dati (in formato cartaceo) riguardanti lo stato di salute e la vita sessuale non sono custoditi separatamente da tutti gli altri documenti.	Basso	Tali dati non sono trattati dall' istituzione scolastica. Nel caso in cui siano consegnati dati non dovuti, essi saranno conservati separatamente fino alla loro distruzione o restituzione

9 Piano di adozione e verifica delle misure di sicurezza

9.1 Verifica delle misure previste dal Disciplinare tecnico

Codice misura	Misura di sicurezza	Stato di adozione	Note
Sistema di autenticazione informatica			
MS-01	Procedura di autenticazione	Adottata	
MS-02	Credenziali di autenticazione	Adottate	
MS-03	Assegnazione individuale delle credenziali.	Adottata	
MS-04	Istruzioni per la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato	Adottata	Sono state fornite adeguate istruzioni scritte agli incaricati del trattamento.
MS-05	Lunghezza, robustezza e modifica della parola chiave.	Adottata	
MS-06	Assegnazione univoca del codice.	Adottata	
MS-07	Disattivazione credenziali non utilizzate.	Adottata	
MS-08	Disattivazione credenziali per perdita della qualità.	Adottata	
MS-09	Istruzioni sulla custodia dello strumento elettronico.	Adottata	Sono state fornite adeguate istruzioni scritte agli incaricati del trattamento.
MS-10	Disposizioni per la custodia delle credenziali.	Adottata	
Sistema di autorizzazione			
MS-12	Sistema di autorizzazione.	Adottato	
MS-13	Profilazione degli incaricati.	Adottato	
MS-14	Verifica periodica dei profili di autorizzazione.	Adottato	
Altre misure di sicurezza			
MS-15	Individuazione periodica degli incaricati.	Adottata	
MS-16	Attivazione e aggiornamento di strumenti idonei a proteggere i dati contro il rischio di intrusione e dall'azione di programmi di cui all'art. 615/quinques del C.P.	Adottata	
MS-17	Prevenzione delle vulnerabilità.	Adottata	
MS-18	Istruzioni organizzative e tecniche per il salvataggio dei dati.	Adottata	Sono state fornite adeguate istruzioni a tutte le figure preposte ai trattamenti
Redazione del documento programmatico della sicurezza			
MS-19	Redazione del documento programmatico.	Adottata	

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari			
MS-20	Protezione dei dati sensibili o giudiziari contro l'accesso abusivo, di cui all' art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.	Adottata	Protezione tramite password di lettura
MS-21	Custodia dei supporti rimovibili.	Adottata	Sono state fornite adeguate istruzioni scritte agli incaricati del trattamento.
MS-22	Regole per la distruzione o la riutilizzazione dei supporti rimovibili.	Adottate	Sono state fornite adeguate istruzioni scritte agli incaricati del trattamento
MS-23	Ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici.	Adottata	
MS-24	Separazione o cifratura dei dati a rivelare lo stato di salute e la vita sessuale per gli organismi sanitari e gli esercenti le professioni sanitarie. Trattamento, trasferimento e trasporto dei dati genetici	Non necessaria	Questa tipologia di dati non è trattata dall'istituzione scolastica
Misure di tutela e garanzia			
MS-25	Dichiarazioni di conformità.	Adottata	I soggetti esterni coinvolti nell'implementazione delle misure minime di sicurezza, rilasciano apposità dichiarazione di conformità al disciplinare tecnico.
MS-26	Redazione del DPS nella relazione accompagnatoria al bilancio.	Adottata	
Trattamenti senza l'ausilio di strumenti elettronici			
MS-27	Istruzioni scritte per gli incaricati finalizzate al controllo ed alla custodia degli atti e dei documenti contenenti dati personali.	Adottate	
MS-28	Aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati.	Adottata	
MS-29	Controllo dell'accesso agli archivi contenenti dati sensibili o giudiziari.	Adottata	

9.1.1 Piano di verifica periodica

Verifiche periodiche previste dal Disciplinare tecnico in materia di misure minime di sicurezza per le diverse tipologie di dati.

Nella tabella sono indicati anche il Riferimento al comma del disciplinare tecnico (Rif. D.T.) e la figura alla quale è affidato il compito di verifica.

Misura	Descrizione	Tipologia di dati	Cadenza	Rif. D.T.	Assegnata a:
(ii) Trattamento con l'ausilio di strumenti elettronici					
Credenziali di autenticazione	disattivazione in caso di mancato utilizzo dei medesimi per un periodo superiore ai 6 mesi	Tutti i dati	6 mesi	7	Amministratore di sistema
Parola chiave	per il trattamento di dati personali deve essere modificata ogni sei mesi	Dati comuni	6 mesi	5	Utenti - Amministratore di sistema
	per il trattamento di dati sensibili deve essere modificata ogni tre mesi	Dati sensibili e giudiziari	3 mesi	5	Utenti - Amministratore di sistema
Profili di autorizzazione	verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione e aggiornare la lista degli incaricati autorizzati	Tutti i dati	1 anno	14 15	Responsabili del trattamento
Antivirus	efficacia ed aggiornamento sono verificati con cadenza almeno trimestrale.	Tutti i dati	3 mesi	16	Amministratore di sistema
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici	Dati comuni sensibili e giudiziari	6 mesi	17	Amministratore di sistema
Backup	salvataggio dei dati con frequenza settimanale	Tutti i dati	7 giorni	18	Amministratore di sistema
DPS	documento programmatico sulla sicurezza	Dati sensibili e giudiziari	1 anno (entro il 31/03 di ogni anno)	19	Titolare o Responsabile
(iii) Trattamento senza l'ausilio di strumenti elettronici					
Profili di autorizzazione	Individuazione dell'ambito del trattamento consentito agli incaricati, individuati anche per classi omogenee	Tutti i dati	1 anno	27	Responsabili del trattamento

Si sottolinea inoltre che:

Le credenziali di autenticazione devono essere immediatamente disattivate in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali (licenziamento, cambio di mansione, pensione ecc.) – (Rif. D.T. – 8).

L'operazione, pur compiuta dall'amministratore di sistema, deve essere stimolata da idonea e tempestiva segnalazione da parte del responsabile del trattamento o da un incaricato da questi specificatamente delegato a questa mansione.

Il codice per l'identificazione, una volta assegnato, non può essere più assegnato ad altri incaricati. Il compito di questa verifica spetta all'amministratore di sistema. (Rif. D.T. – 6)

10 Piano di formazione e di sensibilizzazione

Il piano di formazione e sensibilizzazione, è stato attuato in prima istanza tramite indicazioni di servizio fornite verbalmente, dove sono state illustrate dal Dirigente e dal DSGA le problematiche relative alla privacy e le novità introdotte dal codice.

Per tutto il personale è stata messa e rimane disposizione la normativa relativa al nuovo codice, per il personale ATA verrà utilizzata ai fini formativi la piattaforma EDU.

Viene inoltre messa a disposizione una copia del CD predisposto dal MIUR sul tema della privacy con le seguenti modalità: una copia per la segreteria**,** una copia in Biblioteca e per ogni laboratorio di informatica, una copia per i collaboratori del Dirigente. Agli incaricati nell'ambito della nomina sono state fornite istruzioni dettagliate in merito alle tipologie dati oggetto dei trattamenti individuati all'interno dell'istituzione scolastica, sono state altresì fornite idonee istruzioni scritte sulle misure di sicurezza cui attenersi per la protezione e la riservatezza dei dati.

La formazione sulla privacy sarà programmata nell'ambito dei corsi di formazione deliberati dal collegio docenti, e riconosciuta previa autocertificazione. Modalità di attuazione: collegamento al sito internet della scuola tramite credenziali di autenticazione, accesso ai contenuti del CD predisposto dal MIUR sulla privacy.

11 Misure da adottare

MISURA	DESCRIZIONE	DATA ADOZIONE PREVISTA
Formazione	Ogni anno va censito il personale nuovo che necessità della formazione. La formazione avverrà tramite collegamento al sito internet, dove verrà attuata tramite il CD predisposto dal MIUR sulla privacy e previa autocertificazione.	Entro Dicembre 2011
Protezione locali	Nelle sedi con archivi sprovvisti di rilevatori di fumo e con locali sprovvisti di sistema di antifurto saranno innoltrate ai comuni di competenza le richieste per installarli.	Entro giugno 2011

12 Allegati

Allegato A: Elenco Trattamenti

Allegato B: Informativa

Allegato B bis: istruzioni al personale

Allegato C: Elenco norme dati sensibili

Allegato D: Banche dati

Allegato E: Descrizione sistema informatico

Allegato F: Descrizione locali

Allegato G: Elenco Software utilizzato

Allegato H: Richiesta diffusione esiti scolastici

Allegate lettere di Nomina

Allegate istruzioni date agli incaricati

Allegata modulistica

Allegata copia del D.Lgs 196 30/06/2003 aggiornato

Allegata copia del Regolamento sul trattamento dei dati sensbili e giudiziari emanato dal M.P.I.