Prot 1700/1.4.d
5 GIUGNO 2017

ISTITUTO COMPRENSIVO STATALE DI VERTOVA
SCUOLA DELL'INFANZIA - SCUOLA PRIMARIA - SCUOLA SECONDARIA DI PRIMO GRADO
Via S. Carlo 24029 Vertova (BG) Tel. 035711142 Fax 035738414

Documento programmatico sulla sicurezza D. Lgs. 196/2003 "Codice in materia di protezione dei dati personali"

Luogo e data	Vertova, 10/05/2017
Approvazione	Titolare del trattamento Responsabile al trattamento dei dati
Revisione	13
Principali modifiche dalla revisione precedente	-

Sommario

1 - FINALITA' DEL PRESENTE DOCUMENTO

Il presente documento è redatto ai sensi e per gli effetti del D.Lgs. 196/2003, recante disposizioni inerenti all'adozione delle misure minime di sicurezza, nel trattamento dei dati personali e personali sensibili.

2 - DESCRIZIONE DELL'ISTITUTO

L'Istituto Comprensivo di Vertova una scuola che comprende la scuola per l'infanzia, la scuola primaria e la scuola secondaria di primo grado.

3 - INFORMAZIONI NECESSARIE RELATIVE AL PIANO SICUREZZA

Poiché l'allegato B del decreto legislativo, al comma 19 dispone che:
19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
19.1. l'elenco dei trattamenti di dati personali;
19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
19.3. l'analisi dei rischi che incombono sui dati;
19.4. 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;
19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
19.7. 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;
19.8. 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
Si evidenziano, di seguito, sinteticamente, le informazioni necessarie.

4 - L'ARCHITETTURA DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI

L'architettura di sicurezza è l'insieme di regole, funzioni, strumenti, oggetti e controlli, coerentemente disegnati e resi funzionanti, che garantiscono in ogni struttura organizzativa, ambiente informatico, sistema informativo, singolo elaboratore, il rispetto degli standard di sicurezza definiti dalla struttura economica dell'Istituto.
Gli elementi essenziali di un'architettura sono:

- Funzioni di sicurezza: identificazione e autenticazione degli utenti, controllo accessi ai dati ed alle applicazioni, ecc.
- Meccanismi di sicurezza: i prodotti Hardware e Software che realizzano le funzioni di sicurezza previste nell'architettura.
- Oggetti di sicurezza: oggetti informatici che sono funzionali ai meccanismi di sicurezza tra cui password, liste d'accesso.
- Processi di gestione: insieme dei processi e delle regole per la gestione delle funzioni, dei meccanismi e degli oggetti di sicurezza che fanno parte della architettura (compresi i processi d'allarme e controllo).

5 - ELEMENTI CHE CARATTERIZZANO IL PROGRAMMA D'ADEGUAMENTO, NONCHÉ LE FASI IN CUI ESSO É EVENTUALMENTE RIPARTITO

Come detto il ciclo sicurezza può essere definito nelle seguenti fasi/operazioni:

- organizzazione;
- individuazione informazioni rilevanti;
- analisi dei rischi;
- contromisure possibili;

- definizione della politica dell'Istituto sulla sicurezza;
- realizzazione delle misure decise;
- formazione;
- amministrazione;
- auditing e controlli.

5.1 - ORGANIZZAZIONE

S'intendono gli elementi fondamentali della struttura organizzativa dell'Istituto coinvolti nel trattamento dei dati personali:

- il "titolare del trattamento" dei dati;
- il/i "responsabile/i del trattamento" dati, se esistenti;
- gli "incaricati del trattamento";
- gli incaricati del trattamento dei dati sensibili indicando esplicitamente per quali dati è stata concessa l'autorizzazione;
- gli amministratori del sistema informatico nel caso di sistemi in rete;
- gli eventuali prestatori di servizi, nominati eventualmente "responsabili esterni del trattamento" che trattano all'esterno dell'istituto dati per conto dello stesso istituto (consulenti elaborazione paghe, professionisti, società di certificazione del bilancio, società d'assistenza software);
- gli eventuali responsabili per la gestione dei salvataggi dei dati personali su supporto informatico.

Questa parte ormai è costruita e sono state create le varie figure della Sicurezza che sono operative.

5.2 - ANALISI DEI RISCHI

Dopo aver identificato gli elementi fondamentali del proprio sistema informatico – identificati nel paragrafo 9.6 – con particolare riguardo agli aspetti hardware, si è passati a questa fase che, ormai ultimata, ha portato ad effettuare l'inventario del dati da proteggere, ed alla valutazione dei rischi cui sono soggetti.
L'analisi dei rischi è stata condotta per fasi. Indichiamo di seguito le fasi principali:

5.2.1 - Fase 1 - Censimento dei trattamenti

E' stato fatto un censimento dei trattamenti effettuati dall'Istituto Comprensivo di Vertova nell'ottica di verificare l'eventuale necessità di una eventuale notificazione al Garante. Sono state esaminate le applicazioni software esistenti, e sulla base dei dati gestiti dalle applicazioni stesse, se esse trattano, anche potenzialmente dati personali secondo, quanto previsto dal D.Lgs. 196/2003.
Sono state individuate le *"banche dati"* realizzate con le specifiche applicazioni in uso (*ad es. clienti/fornitori; dipendenti; curricula, ecc.*) e le finalità di trattamento.
Analogamente è stata effettuata l'analisi degli archivi cartacei.
Nel paragrafo 9.3 viene riportata una tabella che elenca le banche dati identificate e le relative tipologie in base alla classificazione prevista dal D.Lgs. 196/2003.

5.2.2 - Fase 2 - Censimento delle banche dati e rilevazione dello stato della sicurezza

Il fine di questa fase è importante ottenere le seguenti informazioni:

- dati anagrafici della banca dati;
- caratteristiche generali;
- accesso alla banca dati;
- sicurezza.

Si è fatta la particolare distinzione tra i vari tipi di trattamento, vale a dire:

- mediante il sistema informatico,
- mediante archivi cartacei o equivalenti (nastri, registrazioni, foto).

Sono stati rilevati i dati personali di tipo sensibile trattati mediante il sistema informatico e mediante archivi cartacei.

5.2.3 - Fase 3 – Analisi dei rischi

Questa fase rappresenta il nucleo fondamentale del piano sicurezza, poiché sulla base di questa valutazione si possono individuare le specifiche azioni da intraprendere. Basandosi su una metodologia semplificata, ed adattata alle specifiche esigenze del D.Lgs. 196/2003, è stata effettuata un'analisi dei rischi, cui sono soggette le banche dati censite. Tale analisi ha permesso di individuare le aree di maggiore rischio e di definire le priorità di intervento.
Si è potuto identificare la classe di "rischio informatico" in base alla struttura del sistema informatico ed al tipo di dati personali trattati.
Tale analisi viene riportata nei punti di controllo presenti nel presente documento nel capitolo 7.

5.3 - LE CONTROMISURE

Sono state definite dando priorità assoluta a quelle previste dal D.Lgs. 196/2003. Come esposto in precedenza l'analisi si è svolta preliminarmente con riferimento alla situazione dell'Istituto e successivamente individuando le misure di sicurezza adottate/da adottare:

- modalità di esecuzione delle misure di sicurezza minime previste dal D.Lgs. 196/2003;
- criteri tecnici ed organizzativi per la protezione delle aree e dei locali e procedure di controllo per l'accesso;
- criteri e procedure per assicurare l'integrità dei dati;
- criteri e procedure per la sicurezza delle trasmissioni dei dati e per le restrizioni di accesso.

5.4 - DEFINIZIONE DELLA POLITICADELL'ISTITUTO SULLA SICUREZZA

È la fase più importante. È il momento in cui si è in grado di definire le regole fondamentali di sicurezza per le banche dati con dati personali.
E' fondamentale che si prenda atto dei rischi e si definisca un'adeguata risposta in termine di politica dell'Istituto (regole, organizzazione, responsabilità, ecc.) e relativi budget di spesa. Il bilanciamento costi-benefici e l'accettazione dei rischi residui, sono parte non rinunciabile di questa fase. Il risultato concreto è la costruzione dello standard dell'Istituto di sicurezza.

5.5 - FORMAZIONE

È un elemento determinante; senza una cultura ed una preparazione degli incaricati il piano sicurezza rischia di non essere efficace.

5.6 - AMMINISTRAZIONE

Sicurezza vuol dire regole, vincoli, controlli, liste di accesso, permessi; ciò comporta una certa dose di inevitabile burocrazia e di lavoro amministrativo. Senza l'attività di amministrazione, dopo qualche tempo, il sistema di sicurezza si degrada e fallisce i suoi obiettivi.

5.7 - AUDITING E CONTROLLI

Costruire un sistema di sicurezza senza, in qualche modo, verificarne l'efficacia, serve a poco. I sistemi informatici sono normalmente molto complessi (sistemi operativi, applicazioni, banche dati, reti, ecc.) e solo con test accurati si può avere una ragionevole certezza di aver costruito un sistema privo di lacune o manchevolezze. Ovviamente non possiamo limitarci ai test iniziali, ma questi vanno ripetuti periodicamente.
Con ciò il ciclo è concluso. Ovviamente, poiché difficilmente i sistemi informativi e l'ambiente in cui operano sono statici, il ciclo della sicurezza non termina mai. E' necessario che almeno una volta l'anno si effettui una revisione dei rischi e, se necessario, anche delle altre fasi, fermo restando le scadenze imminenti previste dalla normativa.

6 - LINEE GUIDA PREVISTE PER DARE PIENA ATTUAZIONE ALLE MISURE MINIME DI SICUREZZA

Occorre distinguere i vari archivi in base alla modalità di trattamento. Occorre, infatti, distinguere:

- I dati personali per i quali il trattamento è eseguito con strumenti diversi da quelli elettronici o comunque automatizzati,
- I dati personali per i quali il trattamento è eseguito con strumenti elettronici o comunque automatizzati.

Per i dati personali per i quali il trattamento è eseguito con strumenti diversi da quelli elettronici o comunque automatizzati il sistema sicurezza dovrà essere caratterizzato dall'osservanza almeno delle seguenti modalità:

- Nel designare gli incaricati del trattamento per iscritto e nell'impartire le istruzioni agli incaricati del trattamento, dovrà

essere prescritto che gli stessi abbiano accesso ai soli dati personali la cui conoscenza sia strettamente necessaria per adempiere ai compiti loro assegnati;

- Occorre disporre che gli atti e i documenti contenenti i dati dovranno essere conservati in archivi ad accesso selezionato e, se affidati agli incaricati del trattamento, dovranno essere da questi ultimi conservati e restituiti al termine delle operazioni affidate. Dovranno quindi essere precisate anche le regole e le procedure per l'accesso selezionato.

Nel caso di trattamento di dati sensibili, di cui all'Art. 4, comma 1, lettera D) del D.Lgs. 196/2003, oltre a quanto appena sopra previsto, devono essere osservate almeno le seguenti modalità:

- Se i documenti contenenti i dati predetti saranno affidati agli incaricati del trattamento, dovrà essere precisato agli incaricati stessi che gli atti e i documenti contenenti i dati dovranno essere conservati in modo da garantirne un accesso controllato e autorizzato;
- L'accesso agli archivi dei documenti contenenti i dati predetti dovrà essere controllato e, nel caso in cui, dopo l'orario di chiusura degli archivi stessi, fosse consentito a qualche incaricato o terzo autorizzato l'accesso agli archivi medesimi, occorre prevedere una procedura che preveda preventivamente che i soggetti ammessi siano identificati e registrati.

I supporti non informatici contenenti la riproduzione di informazioni relative al trattamento di dati personali sensibili e giudiziari, devono essere conservati e custoditi con le modalità sopra esposte.
Per il trattamento dei dati personali effettuato con elaboratori occorre prevedere, anteriormente all'inizio del trattamento, almeno le seguenti misure:

- Una parola chiave per l'accesso ai dati, fornita agli incaricati del trattamento, i quali possono in maniera autonoma e senza intervento di soggetti tecnicamente competenti, sostituirla in caso di scadenza della validità della stessa o in caso di violazioni della sicurezza.
- Individuare per iscritto, quando vi è più di un incaricato del trattamento e sono in uso più parole chiave, i soggetti preposti alla loro custodia o che hanno accesso ad informazioni che concernono le medesime.
- A ciascun utente o incaricato del trattamento deve essere attribuito un codice identificativo personale (ID USER) per l'utilizzazione dell'elaboratore; uno stesso codice, fatta eccezione per gli amministratori di sistema relativamente ai sistemi operativi che prevedono un unico livello di accesso per tale funzione, non può, neppure in tempi diversi, essere assegnato a persone diverse;
- I codici identificativi personali (ID USER), devono essere assegnati e gestiti, in modo che ne sia prevista la disattivazione, in caso di perdita della qualità che consentiva l'accesso all'elaboratore, o di mancato utilizzo dei medesimi, per un periodo superiore ai sei mesi.

Gli elaboratori, devono essere protetti da "software antivirus" idoneo contro il rischio di intrusione, ad opera di programmi di cui all'art. 615 quinquies del codice penale. L'efficacia e l'aggiornamento di detti programmi ANTIVIRUS dovranno essere verificati con cadenza almeno semestrale.
La Regola 17 dell'All. B del D. Lgs. 196/03 prevede che: "gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.". E' stato definito un piano di controlli con cadenza almeno semestrale per verificare l'installazione sugli elaboratori degli aggiornamenti volti a limitare le vulnerabilità esposte nel paragrafo precedente.
Per essere precisi evidenziando che le disposizioni di cui alle precedenti punti, non si applicano al trattamento dei dati personali di cui, ai sensi del D.Lgs. n. 196/2003, è consentita la diffusione.
Nei casi in cui con elaboratori accessibili in rete vi sia il trattamento dei dati sensibili, l'accesso per effettuare le operazioni di trattamento deve essere determinato sulla base di autorizzazioni assegnate, singolarmente o per gruppi di lavoro, agli incaricati dei trattamento o della manutenzione.
Periodicamente, e comunque almeno una volta l'anno, dovrà essere verificata la sussistenza delle condizioni per la conservazione delle singole autorizzazioni in essere.
Nel caso di trattamento dei dati sensibili effettuato con elaboratori accessibili in rete, i supporti già utilizzati per il trattamento possono essere riutilizzati qualora le informazioni precedentemente contenute non siano tecnicamente in alcun modo recuperabili, altrimenti devono essere distrutti.
Nel caso di effettuazione di trattamenti dei dati mediante gli elaboratori in rete la normativa prevede l'obbligo di predisposizione e aggiornamento, con cadenza annuale, del documento programmatico sulla sicurezza del dati (DPS) per definire, sulla base dell'analisi dei rischi, della distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati stessi.
L'efficacia delle misure di sicurezza adottate in base al documento stesso dovrà essere oggetto di controlli periodici, da eseguirsi con cadenza almeno annuale.

7 - MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

S'illustra, in sintesi, con quale modalità le misure minime di sicurezza, previste per le diverse classi o categorie di rischio, sono state realizzate nella realtà tecnologica ed organizzativa dell'Istituto.
Il trattamento dei dati personali per il sistema informativo dell'Istituto può essere classificato nelle seguenti casistiche:

- Archivi con trattamento MANUALE *(per le relative misure si rinvia alla sezione A)*
- Archivi con trattamento tramite elaboratori IN RETE *(per le relative misure si rinvia alla sezione B)*

La descrizione dello stato di adozione delle misure di sicurezza indicate è espressa mediante uno stato di conformità. La legenda degli stati è la seguente:

- OK: la misura di sicurezza è presente nella gestione del rischio;
- NC: la misura di sicurezza non è presente nella gestione del rischio;
- I/A: l'attuazione della misura di sicurezza è in fase di termine;
- N/A: la misura di sicurezza non è applicabile alla situazione presente di gestione del rischio;
- ADN: aspetti degni di nota; attestazione rilevate durante l'analisi che rispecchiano particolare attenzione alla definizione di misure di sicurezza che superano gli standard della normativa;
- ADM: azioni di miglioramento; suggerimenti o indicazioni utili per raggiungere gli standard di sicurezza imposti dalla normativa quali le misure minime o idonee.

7.1 - ARCHIVI CON TRATTAMENTO CARTACEO

7.1.1 - Definizione della figura di titolare del trattamento dei dati

Individuazione del titolare del trattamento.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'individuazione del titolare del trattamento è riportata nella sezione dei dettagli del piano di intervento.

7.1.2 - Definizione della figura di responsabili interni ed esterni

Individuazione del responsabile interno del trattamento e dei responsabili dei trattamenti esterni identificati.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'individuazione dei responsabili del trattamento è riportata nella sezione dei dettagli del piano di intervento. È presente in sede l'evidenza dell'invio delle lettere di nomina ai responsabili esterni al trattamento dati. E' stata nominata la figura di responsabile al trattamento dei dati con una apposita nomina da parte della Dirigente.

7.1.3 - Conservazione documenti con dati personali ordinari

In archivi ad accesso selezionato.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				In tutte le strutture dell'istituto i dati personali sono custoditi negli uffici di competenza. L'ufficio di gestione dati operativi è unico e tutti gli operatori hanno pieno accesso dato la competenza sui dati.

7.1.4 - Conservazione documenti con dati sensibili

In archivi ad accesso selezionato e supervisionato da parte del personale incaricato in modo specifico.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'archivio attuale delle schede del personale interno e quelle degli alunni con dati sensibili è custodito in archivi muniti di serratura e sotto la custodia del personale incaricato della segreteria.

7.1.5 - Modalità organizzazione archivi

Procedure e modalità per l'organizzazione degli archivi cartacei ad accesso selezionato.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				In tutti i dipartimenti dell'istituto l'organizzazione degli archivi permette la facile rintracciabilità dei dati. Esiste un archivio storico condiviso a cui ha accesso solo il personale di segreteria che ne ha competenze.

7.1.6 - Criterio di accesso ai dati

Specifica necessità del trattamento

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'accesso ai dati personali gestiti dagli uffici è controllato da parte del personale incaricato.

7.1.7 - Accesso agli archivi con Dati Sensibili

Accesso selezionato e controllato da parte dei soli incaricati addetti.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'archivio attuale delle schede del personale interno e degli alunni con dati sensibili è custodito in archivi muniti serratura. Esiste una procedura non scritta che regolamenta l'accesso a questi dati da parte degli interessati.

7.1.8 - Modalità di registrazione degli accessi ai dati sensibili fuori dall'orario normale

Identificare i soggetti esterni all'Istituto che possono accedere alla strutture in assenza degli incaricati nominati.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Non è configurata la situazione di accesso alle strutture al di fuori degli orari di ufficio da parte di personale esterno. E' stato predisposto il registro di accesso alle strutture da parte di personale non incaricato in modo specifico. E' stato aggiornato il registro di accesso alle strutture a seguito di nuovo personale.

7.1.9 - Documenti con dati personali ordinari affidati agli incaricati

Comunicare agli incaricati che essi vanno conservati e restituiti al termine delle operazioni affidate

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stata erogata formazione al personale non docente su procedure di gestione della documentazione cartacea. E' stata definita la procedura per la formazione del personale docente mediante consegna di materiale e firma di un documento per presa visione.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
				E' stata aggiornata la consegna dei documenti a seguito di nuovo personale.

7.1.10 - Documenti con dati sensibili affidati agli incaricati

Comunicare agli incaricati che devono essere conservati, fino alla loro restituzione, in maniera che ad essi non accedano persone prive di autorizzazione

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stata erogata formazione al personale non docente su procedure di gestione della documentazione cartacea. E' stata definita la procedura per la formazione del personale docente mediante consegna di materiale e firma di un documento per presa visione. E' stata aggiornata la consegna dei documenti a seguito di nuovo personale.

7.1.11 - Riepilogo risultati archivi a trattamento manuale

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
10	0	10	10	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.2 - ARCHIVI CON TRATTAMENTO CON ELABORATORI IN RETE

7.2.1 - Incaricati individuati per iscritto

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stata completa la nomina degli incaricati mediante incarichi scritti. Tale procedura viene mantenuta nel tempo attraverso la creazione di materiale standard per la gestione delle assunzioni.

7.2.2 - Custodi parole chiave se nominato va individuato per iscritto

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				La scelta delle password spetta all'incaricato. Esiste una figura di custode delle password all'interno della struttura. Tale soggetto ha la custodia delle buste in cui gli incaricati con strumento informatico inseriscono la propria password all'atto della modifica.

7.2.3 - Amministratore di sistema se nominato va individuato per iscritto

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'istituto si affida per la gestione della rete informatica ad un fornitore dell'hardware e del software esterno. E' stata sottoscritta la lettera di nomina dell'amministratore di sistema.

7.2.4 - Registro degli accessi da parte dell'Amministratore di sistema

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stato definito il sistema di creazione del registro degli accessi così come previsto dal provvedimento del Garante del 27/11/2008. Visti gli interventi limitati alla rete informatica si è stabilito che ad ogni intervento verrà chiesto di sottoscrivere un rapportino cartaceo.

7.2.5 - Accesso ai dati, parola chiave

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Le password sono presenti in accesso alle singole postazioni.

7.2.6 - Regole per le modalità di attivazione, variazione e gestione delle parole chiave per l'accesso ai dati personali

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stato completato il processo di adeguamento delle postazioni di rete, escluse le postazioni di amministrazione e di gestione del personale interno, secondo i nuovi standard della normativa che per comodità sono riportati: *la parola chiave è composta da almeno otto caratteri* oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi. Il cambio della password delle postazioni avviene ogni 3 mesi e viene gestito dal server. Gli utenti registrano poi la propria password in una busta chiusa consegnata poi al soggetto nominato per la custodia.

7.2.7 - Sostituzione parola chiave, autonoma ove tecnica possibile

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stato completato il processo di informazione degli utenti della rete della norma di gestione della password, attraverso la firma di un documento all'atto dell'assunzione.

7.2.8 - Blocco della postazione operativa in caso di assenza dell'operatore

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stato impostato su tutte le postazioni operative della rete informatica un sistema che blocca la postazione e ne richiede lo sblocco mediante password in caso di assenza dell'operatore.

7.2.9 - Codice identificativo personale (primo elemento dei criteri di autenticazione)

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' inserito su tutte le postazioni dato che i sistemi operativi delle postazione hanno tutte questa possibilità.

7.2.10 - Criterio di assegnazione e revoca User ID, assegnamento delle credenziali secondo la necessità di trattamento da parte degli incaricati nominati

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'organizzazione dei file del sistema è definita secondo le competenze degli utenti. L'organizzazione degli accessi al sistema gestionale rispecchia le competenze degli utenti.

7.2.11 - Validità User ID, massimo 6 mesi di non utilizzo

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'utenza che viene dismessa viene subito disattivata secondo delle procedure definite in carico alla gestione del personale anche se non formalizzata.

7.2.12 - Rischio di intrusione (antivirus) programmi di protezione adeguati

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Esiste un anti virus installato su tutte le postazioni. Il sistema installato è F-Secure.

7.2.13 - Fissazione criteri di utilizzo e di aggiornamento dei programmi antivirus

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Le postazioni si aggiornano in modo automatico dal sito del produttore. L'aggiornamento della versione dell'anti virus viene effettuata dal tecnico dell'assistenza allo scadere delle licenze.

7.2.14 - Verifica di efficacia programmi di protezione: semestrale

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				I pacchetti di anti virus sono aggiornati alla scadenza. Il tecnico hardware ha il compito di effettuare gli aggiornamenti alla scadenza.

7.2.15 - Aggiornamento programmi di protezione, semestrale

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				L'aggiornamento è effettuato presso il sito del produttore.

7.2.16 - Installazione di aggiornamenti volti a prevenire la vulnerabilità degli strumenti elettronici

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' definita una procedura di controllo delle postazioni e dei server in carico all'amministratore di sistema che provvede all'installazione di tali aggiornamenti ove necessario. Tale procedura è automatizzata sulle singole postazioni ma è lasciato all'utente effettuare installazioni aggiuntive oltre al controllo dell'amministratore di sistema.

7.2.17 - Riepilogo risultati archivi a trattamento informatico

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
16	0	16	16	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.3 - PROCEDURE TECNICHE ED ORGANIZZATIVE PER LA PROTEZIONE FISICA DELLE AREE E DEI LOCALI INTERESSATI DALLE MISURE DI SICUREZZA.

7.3.1 - Localizzazione e limitazioni all'accesso del server

Conformità				*Evidenze della verifica e note*
OK	*NC*	*I/A*	*N/A*	
X				Non è prevista una sala server dedicata; il server è collocato in un ufficio custodito dal personale incaricato.

7.3.2 - Sistemi di registrazione degli accessi e delle uscite dei dipendenti e del personale esterno

Conformità				*Evidenze della verifica e note*
OK	*NC*	*I/A*	*N/A*	
			X	L'accesso ai luoghi di custodia dei sistemi non è registrato.

7.3.3 - Sistemi di chiusura dei locali, sia in generale, sia nello specifico dei locali ove sono custoditi i sistemi

Conformità				*Evidenze della verifica e note*
OK	*NC*	*I/A*	*N/A*	
			X	I sistemi sono custoditi in una sala custodita da parte del personale interno in modo costante.

7.3.4 - Presenza di un custode

Conformità				*Evidenze della verifica e note*
OK	*NC*	*I/A*	*N/A*	
			X	Non è presente un custode.

7.3.5 - Esistenza di un servizio di vigilanza esterna

Conformità				*Evidenze della verifica e note*
OK	*NC*	*I/A*	*N/A*	
			X	Non esiste un servizio di vigilanza sulla struttura.

7.3.6 - Dispositivi antincendio (estintori, manichette, impianti di rilevazione di spegnimento automatico)

Conformità				*Evidenze della verifica e note*
OK	*NC*	*I/A*	*N/A*	
X				E' presente un sistema antincendio nella struttura.

7.3.7 - Dispositivi anti intrusione (specifici o generali per tutto l'edificio/stabilimento)

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non è presente questa misura di sicurezza.

7.3.8 - Custodia in armadi o classificatori non accessibili

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	La misura di sicurezza è ritenuta troppo dispendiosa per il livello di rischio a cui sono esposti gli archivi di dati personali. Esiste un armadio chiuso solo per gli apparati di rete.

7.3.9 - Modalità di custodia delle chiavi

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non è definita una modalità precisa di custodia dato che i sistemi sono in una stanza chiusa a chiave sotto il controllo dell'incaricato dell'amministrazione.

7.3.10 - Riepilogo risultati protezione fisica delle aree interessate dalle misure di sicurezza

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
9	7	2	2	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.4 - PROCEDURE PER ASSICURARE L'INTEGRITÀ DEI DATI: BACKUP

7.4.1 - Procedure per l'esecuzione dei backup

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Sono previsti i seguenti backup dei dati così come segnalato dalla società informatica: **Backup Server**: Esecuzione:tutti i giorni alle 17:00, su disco di rete - Tipo di Backup: Immagine disco Backup completo di tutti i dischi del server. Gestione completamente automatizzata e trasparente. **Backup Dati** Esecuzione: tutti i giorni alle 20:00, su disco di rete - Tipo di Backup: Archivio compresso Backup di documenti e file in uso dagli utenti. La procedura prevede che del mese corrente siano mantenuti sempre i backup degli ultimi 7 giorni. Viene inviata giornalmente una e-mail che segnala se il backup è stato effettuato correttamente. **Backup Sissi** Esecuzione: ogni 30gg, su disco di rete - Tipo di Backup: Archivio compresso Il salvataggio viene effettuato manualmente in remoto da un operatore CONSINFO. **RAID 1** Una copia identica e istantanea dei dati su due dischi rigidi differenti, gestita in modo completamente trasparente.

7.4.2 - Procedure per l'archiviazione dei backup

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Le copie sono tenute in una zona differente rispetto al server.

7.4.3 - Tipi e numeri di copie dei backup eseguiti

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Vedere la descrizione 7.4.1.

7.4.4 - Utilizzo di casseforti o armadi ignifughi per l'archiviazione dei backup

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non è prevista questa misura di sicurezza.

7.4.5 - Criteri di rotazione dei dispositivi e di eliminazione dei dispositivi obsoleti

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Vedere la descrizione 7.4.1.

7.4.6 - Procedure per la verifica della registrazione dei backup

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Vedere la descrizione 7.4.1.

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

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Il responsabile del sistema di salvataggio è stato definito.

7.4.8 - Riepilogo risultati procedure per assicurare l'integrità dei dati

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
7	0	7	7	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.5 - PROCEDURE PER ASSICURARE L'INTEGRITÀ DEI DATI: EVENTUALI ALTRE MISURE

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

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' presente un sistema di controllo dell'alimentazione che verifica il server.

7.5.2 - Climatizzazione dei locali

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	

7.5.3 - Divieto di installare software non autorizzato dall'istituto (rischi virus, conflitti tra applicazioni)

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stata effettuata l'operazione di informare tutti gli incaricati circa le responsabilità a loro carico dell'utilizzo delle postazioni di lavoro, del software, e degli strumenti installati, che possono far correre rischi non prevedibili agli archivi di dati (sensibili o meno).

7.5.4 - Piano di disaster recovery

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Non è previsto un piano di disaster recovery.

7.5.5 - Procedure di riutilizzo controllato dei supporti di memorizzazione

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' previsto un sistema di controllo dei supporti rimovibili.

7.5.6 - Riepilogo risultati altre misure per assicurare l'integrità dei dati

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
5	1	4	4	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.6 - PROCEDURE PER LA SICUREZZA DELLE TRASMISSIONI DEI DATI E PER LE RESTRIZIONI DI ACCESSO

7.6.1 - Firewall software o hardware

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Dato il sistema di collegamento con internet sempre attivo potrebbe essere effettuata l'installazione di un sistema firewall software sulle singole postazioni.

7.6.2 - Limitazioni di routing

Definizione di regole di utilizzo dello strumento internet da parte degli incaricati al trattamento mediante limitazione delle funzioni di navigazione delle postazioni di rete.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non sono presenti limitazioni sull'uso della rete internet.

7.6.3 - Disposizioni organizzative di limitazione dell'utilizzo di internet

Prescrizioni sull'utilizzo della rete internet e della posta elettronica da inserire nelle istruzioni scritte dagli incaricati.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Potrebbe essere effettuata l'operazione di informare tutti gli incaricati circa le responsabilità a loro carico dell'utilizzo degli strumenti di comunicazione installati, che possono far correre rischi non prevedibili agli archivi di dati (sensibili o meno). E' stata effettuata la predisposizione della lettera sul corretto utilizzo di internet a tutto il personale dipendente.

7.6.4 - Controlli sui software di comunicazione sui computer degli utenti

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Gli accessi dall'esterno al sistema informativo sono presenti con sistemi di controllo di accesso mediante programmi di controllo remoto che utilizzano connessioni protetto da protocolli di crittografia.

7.6.5 - Sicurezza delle connessioni mediante reti senza fili

La presenza di connessioni di rete senza fili (wireless) deve essere messa in sicurezza mediante password di accesso complesse e conosciute solo al personale di ufficio.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				Le connessioni di rete presenti nell'Istituto sono sia cablate che senza fili. Le reti senza fili sono realizzate

Conformità				*Evidenze della verifica e note*
OK	*NC*	*I/A*	*N/A*	
				mediante access point dedicato con sistema di accesso sicuro protetto mediante password di accesso. Le reti senza fili presenti non permettono l'accesso alle postazioni della rete di segreteria.

7.6.6 - Riepilogo risultati sicurezza delle trasmissioni dati

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
5	1	4	4	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.7 - PROCEDURE PER LA SICUREZZA DEI DATI TRATTATI SU ALTRI SUPPORTI: VIDEOSORVEGLIANZA

7.7.1 - Informative delle altre tipologie di trattamento

Verifica sulla locazione fisica degli impianti della presenza di informative adeguate della presenza del trattamento. Installazione di cartellonistica.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non sono presenti impianti di videosorveglianza.

7.7.2 - Verifica delle conformità del trattamento rispetto alle linea guida della normativa

Definizione di regole di utilizzo dello strumento videosorveglianza da parte degli incaricati specifici mediante procedure, anche tecniche, di utilizzo degli strumenti di trattamento.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non sono presenti impianti di videosorveglianza.

7.7.3 - Definizione delle motivazioni del trattamento

Definizione, mediante atto scritto, delle motivazioni per cui è presente il sistema di trattamento.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non sono presenti impianti di videosorveglianza.

7.7.4 - Definizione tecnica della tipologia di trattamento

Definizione, mediante atto scritto, delle procedure di trattamento con particolare attenzione alla descrizione tecnica dei sistemi di trattamento.

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non sono presenti impianti di videosorveglianza.

7.7.5 - Riepilogo risultati sicurezza dei dati trattati su altri supporti: videosorveglianza

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
4	4	0	0	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.8 - ALTRE MISURE PREVISTE DAL CODICE

7.8.1 - Invio delle informative a clienti e fornitori

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' presente la procedura formale di sottoscrizione delle informative e consensi al trattamento da parte dei genitori degli alunni al momento della compilazione del modulo di iscrizione all'istituto.

7.8.2 - Raccolta del consenso presso i clienti per le spedizioni di materiale pubblicitario

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Attualmente non è previsto un sistema di spedizione di materiale informativo o pubblicitario ai clienti. I dati dei clienti sono utilizzati unicamente per la gestione del rapporto commerciale e per i relativi obblighi legali.

7.8.3 - Notifica al Garante per i trattamenti previsti dal Codice

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
			X	Non è previsto l'obbligo di notifica dato che le tipologie di trattamento non rientrano nei casi previsti dalla norma.

7.8.4 - Altre misure previste dal codice

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
3	2	1	1	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.9 - PIANI DI FORMAZIONE PER GLI INCARICATI DEL TRATTAMENTO

7.9.1 - Calendario e contenuti degli incontri svolti o previsti

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				La consegna del materiale informativo agli incaricati interni viene effettuato ad intervalli regolari in fase di nomina per i docenti. L'invio del materiale avviene via posta elettronica e la raccolta delle firme per la presa visione viene fatta su apposito modulo.

7.9.2 - Conservazione della documentazione consegnata

Conformità				Evidenze della verifica e note
OK	NC	I/A	N/A	
X				E' stata effettuata la registrazione della consegna della documentazione a tutti gli incaricati.

7.9.3 - Riepilogo risultati piano di formazione

Riepilogo					
Totale misure	*Totale misure non applicate*	*Totale misure applicabili*	*Totale misure applicate*	*In ultimazione*	*Non attuate*
2	0	2	2	0	0

Conformità in %	***In attuazione %***	***Non conformità %***
100	**0**	**0**

Caratteristica	*Evidenze della verifica e note*
ADN	-
ADM	-

7.10 - TABELLA DI RIEPILOGO

Nella tabella sottostante sono inseriti i risultati delle sezioni analizzate nei paragrafi precedenti.

Sezione	*Conformità in %*	*In attuazione in %*	*Non conformità in %*
Archivi con trattamento manuale	100	0	0
Archivi con trattamento con elaboratori in rete	100	0	0
Procedure tecniche ed organizzative per la protezione fisica delle aree e dei locali interessati dalle misure di sicurezza	100	0	0
Procedure per assicurare l'integrità dei dati: backup	100	0	0
Procedure per assicurare l'integrità dei dati: eventuali altre misure	100	0	0
Procedure per la sicurezza delle trasmissioni dei dati e per le restrizioni di accesso	100	0	0
Procedure per la sicurezza dei dati trattati su altri supporti: videosorveglianza	100	0	0
Altre misure previste dal codice	100	0	0
Piano di formazione per gli incaricati al trattamento	100	0	0
Totale	**100**	**0**	**0**

8 - LINEE GUIDA PREVISTE PER PIÙ AMPIE MISURE DI SICUREZZA

Vengono, qui di seguito, esaminate le funzioni di sicurezza che rispondono ai requisiti della maggior protezione rispetto ai minimi della normativa. Quanto si pianificherà di realizzare, sarà definito nel DPS, tenendo presente la realtà dell'Istituto, onde evitare di introdurre meccanismi costosi e inutili per le circostanze, che caratterizzano la nostra struttura.

8.1 - CUSTODIA

Presuppone che siano definiti dei processi (norme e responsabilità) nell'area sia della sicurezza fisica che logica.

8.2 - SICUREZZA FISICA

È importante verificare se solo gli addetti ai lavori (incaricati del trattamento) possano accedere ai locali dei centri di calcolo, e se le altre persone (visitatori, addetti ai lavori ausiliari, ecc.), vi accedano solo con apposita autorizzazione. A tale proposito, la struttura presenta una situazione tale per cui gli ingressi sono sorvegliati e viene eseguita un'identificazione delle persone che vi accedono. Tutte le aperture sono dotate di impianti d'allarmi, per cautelarsi da intrusioni, durante il periodo in cui il centro resta non presidiato.
Per i server dipartimentali è prevista una sala separata dal resto delle aree di lavoro degli operatori. Tale sala viene mantenuta chiusa a chiave e la chiave è in gestione alla segreteria ed al titolare per permettere l'accesso, previa verifica dell'identità, ai soggetti che hanno il compito di manutenere i sistemi che sono collocati all'interno della sala.
Un discorso a parte meritano le *nastroteche* e i punti di conservazione dei dischi; poiché il decreto legge parla di rischi di perdita, anche accidentale, se i nastri o dischi sono unici, opportuni impianti antincendio sono stati installati per evitare ulteriori danni ai nastri, in caso d'utilizzo di dette apparecchiature. Quanto detto per i nastri vale anche per i dischi rimovibili o per i sistemi NAS che sono presenti all'interno della sala server.

8.3 - SICUREZZA LOGICA

I metodi per proteggere le informazioni dal punto di vista logico, sono molti, e fortemente dipendenti dalla tipologia dei sistemi operativi utilizzati (piattaforme Software), anche se con qualche eccezione; di seguito sono elencati i sistemi applicati alla rete informatica dell'Istituto Comprensivo Statale di Vertova:

- Integrità del sistema operativo mediante applicazione delle patch distribuite dai fornitori dei sistemi operativi,
- Accessi discrezionali in funzione della tipologia di utente che richiede l'accesso,
- Classificazione delle informazioni per poter gestire nel migliore dei modi la griglia di accesso ai dati in base alla tipologia di utente identificata al punto precedente,
- Installazione di un sistema Antivirus con controllo centralizzato e con aggiornamento locale su tutte le postazioni della rete informatica.

8.4 - CLASSIFICAZIONE DELLE INFORMAZIONI

Sul piano pratico occorre analizzare se adottare un sistema di classificazione che prevede, per esempio, i dati " sensibili" classificati ad un livello più alto dei dati "personali". L'adozione di un opportuno sistema di classificazione, oltre ad accrescere la protezione dei dati, permetterebbe di adottare un sistema di protezione selettivo. Un esempio potrebbe essere:

- Informazioni "sensibili": altamente riservate,
- Informazioni "private": riservate,
- Altre informazioni dell'Istituto riservate: riservate,
- Altre informazioni dell'Istituto: non classificate.

Un sistema di classificazione, perché sia efficace, deve comprendere anche le informazioni cartacee.

8.5 - METODI D'ACCESSO

Il più usato è quello basato su parole chiave o password. Per accrescerne l'efficacia, occorrono regole precise di gestione delle password. Occorre definirne la lunghezza minima (8 caratteri, ove tecnicamente possibile, per D.Lgs. 196/2003, allegato B, comma 5), la durata e le regole grammaticali, per evitare password facilmente indovinabili. Ogni password dovrebbe essere abbinata ad un individuo; questo è l'unico modo per risalire alle responsabilità d'eventuali azioni contrarie a quanto previsto dal decreto legge.

8.6 - ANTIVIRUS

Nell'architettura di sicurezza dei Personal Computer dovrebbe essere sempre previsto non solo un Antivirus, ma anche, e soprattutto, un rigoroso processo di controllo delle memory stick, chiavette USB, ecc. che entrano nell'Istituto e che si interfacciano con strumentazioni informatiche dell'Istituto e, se collegati ad Internet, del software che è scaricato dalla rete. Tale attività viene garantita dalla presenza di un firewall che impedisce le connessioni non protette a siti non attendibili.
La lista di metodologie di protezione potrebbe continuare, ma riteniamo che quelle richiamate, sono sufficienti per disegnare un'architettura di sicurezza minima. Ovviamente, se le banche dati dovessero essere inserite in un sistema particolarmente esposto, come per esempio un Web di Internet, si pone certamente il problema di attivare un disegno specifico che preveda l'installazione di Firewall e di protocolli di mutuo riconoscimento basati su chiavi crittografiche.

8.7 - CONTROLLI

Controlli periodici:

- Auditing,
- Revisioni interne,
- Test.

Controlli continui:

- Analisi dei log,
- Routine di controllo.

9 - DETTAGLI PIANO INTERVENTO

9.1 - TITOLARI E RESPONSABILI DEL TRATTAMENTO

In questo capitolo sono elencate le figure esposte nel capitolo 5.1 – Organizzazione.

Titolare del trattamento	
Preside:	Elena Margherita Berra
Soggetto:	Istituto Comprensivo di Vertova
Indirizzo:	Via S. Carlo, 29 – Vertova (BG)

Responsabile trattamento dati	
Nome e cognome:	Dentella Adriana
Codice fiscale:	DNTDRN54A54A163Z
In carica presso:	Istituto Comprensivo di Vertova
Indirizzo:	Via S. Carlo, 29 – Vertova (BG)

Responsabile salvataggio dati	
Nome e cognome:	Dentella Adriana
In carica presso:	Istituto Comprensivo di Vertova
Indirizzo:	Via S. Carlo, 29 – Vertova (BG)

Amministratori di sistema	
Nome e cognome:	Mercandelli Sergio
In carica presso:	Punto Sistemi S.r.l.
Indirizzo:	Via Provinciale 114 – 24021 Albino
Nome e cognome:	Piffari Mauro
In carica presso:	Consinfo.it
Indirizzo:	Via Pianoro, 9 – 24029 Vertova

Luoghi di custodia dei dati	
Soggetto:	Istituto Comprensivo di Vertova
Indirizzo:	Via S. Carlo, 29 – Vertova (BG)
Soggetto:	Scuola Elementare di Vertova
Indirizzo:	Via Roma, 18 – Vertova (BG)

Luoghi di custodia dei dati	
Soggetto:	Scuola Elementare di Colzate
Indirizzo:	Via Bonfanti, SNC – Colzate (BG)
Soggetto:	Scuola Materna di Colzate
Indirizzo:	Via Roma, SNC – Colzate (BG)
Soggetto:	Scuola Elementare di Fiorano
Indirizzo:	Via Donizzetti, 19 – Fiorano (BG)

9.2 - ORGANIGRAMMA

Secondo l'art. 19 comma 2 dell'allegato B del D.Lgs. 196/2003 è necessario definire la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati. Di seguito sono elencate le unità organizzative che gestiscono i dati personali nella struttura dell'Istituto.

- Ufficio amministrazione
- Ufficio gestione del personale
- Ufficio programmazione e gestione personale didattico
- Ufficio gestione alunni
- Corpo docente

9.3 - ELENCO DELLE BANCHE DATIE DEI TRATTAMENTI

La presenza all'interno dell'Istituto di un sistema informativo, connesso in rete intranet, la quale fornisce anche la connessione ad Internet illimitata a tutti i client, utilizzata anche per la gestione della posta elettronica, impone di prendere in considerazione il "caso pessimo" di configurazione previsto dal legislatore, almeno per quanto attiene la trattazione dei dati svolta con l'uso di sistemi computerizzati.
La classificazione e la codifica dei trattamenti effettuati è quella definita nelle istruzioni di compilazione alla notifica al trattamento dei dati da parte del Garante della Privacy.
Di seguito viene riportata la tabella che identifica le banche dati classificate nell'Istituto.

Categoria di dati	*Dettaglio categoria*	*Natura dei dati trattati*		
		Personali	*Sensibili*	*Giudiziari*
Clienti e fornitori: dati personali relativi alle società esterne con cui si hanno rapporti commerciali	Anagrafica clienti	X		
	Anagrafica fornitori	X		
	Pratiche clienti	X	X	
	Contratti	X		
	Fatture	X		
	Ordini	X		
	Contenziosi con clienti e fornitori	X		X
Dipendenti: dati personali relativi ai dipendenti dell'Istituto	Dipendenti	X	X	X
	Rilevamento presenze	X		
	Paghe	X	X	
	Visite mediche	X	X	
	Cartelle mediche, infortuni, malattia	X	X	
	Contenzioso con dipendenti	X	X	X

Di seguito viene riportata la tabella che identifica gli accessi che sono possibili alle banche dati in base alla suddivisione delle funzioni dell'Istituto (organigramma).

Categoria di dati	*Dettaglio categoria*	*Unità organizzative coinvolte nel trattamento*
Alunni e fornitori: dati personali relativi alle società esterne con cui si hanno rapporti commerciali	Anagrafica alunni	Ufficio amministrazione Ufficio gestione alunni Corpo docente
	Anagrafica fornitori	Ufficio amministrazione
	Contratti	Ufficio amministrazione Ufficio gestione del personale Ufficio programmazione e gestione personale didattico

	Fatture	Ufficio amministrazione Ufficio gestione del personale Ufficio programmazione e gestione personale didattico
	Ordini	Ufficio amministrazione Ufficio gestione del personale Ufficio programmazione e gestione personale didattico
	Contenziosi con alunni e fornitori	Ufficio amministrazione
	Protocollo riservato	Ufficio presidenza e vice presidenza
Dipendenti: dati personali relativi ai dipendenti dell'istituto	Dipendenti	Ufficio amministrazione Ufficio gestione del personale Ufficio programmazione e gestione personale didattico
	Rilevamento presenze	Ufficio amministrazione
	Paghe	Ufficio amministrazione Ufficio gestione del personale Ufficio programmazione e gestione personale didattico
	Visite mediche	Ufficio amministrazione
	Cartelle mediche, infortuni, malattia	Ufficio amministrazione Ufficio gestione del personale Ufficio programmazione e gestione personale didattico
	Contenzioso con dipendenti	Ufficio amministrazione

In funzione del contenuto dei dati in esame e delle modalità di trattamento di questi, si evidenziano quattro possibili casi:

9.3.1 - Trattamento di dati personali effettuato con strumenti elettronici e/o automatizzati

Gli scopi per cui saranno utilizzati, in conformità al proprio oggetto sociale, sono:

- Trattamento giuridico ed economico del personale
- Reclutamento, selezione, valutazione e monitoraggio del personale
- Formazione professionale
- Adempimento di obblighi fiscali o contabili
- Adempimenti connessi al versamento delle quote di iscrizioni sindacali o all'esercizio dei diritti sindacali
- Igiene e sicurezza sul lavoro
- Programmazione delle attività
- Gestione del patrimonio mobiliare e immobiliare

- Gestione della clientela (amministrazione della clientela; amministrazione di contratti, ordini, spedizioni e fatture; controllo dell'affidabilità e solvibilità)
- Gestione dei fornitori (amministrazione dei fornitori; amministrazione di contratti, ordini, arrivi, fatture)
- Gestione del contenzioso
- Marketing

9.3.2 - Trattamento di dati sensibili effettuato con strumenti elettronici e/o automatizzati

Gli scopi per cui saranno utilizzati, in conformità al proprio oggetto sociale, sono:

- Trattamento giuridico ed economico del personale
- Reclutamento, selezione, valutazione e monitoraggio del personale
- Adempimento di obblighi fiscali o contabili
- Adempimenti connessi al versamento delle quote di iscrizioni sindacali o all'esercizio dei diritti sindacali
- Igiene e sicurezza sul lavoro
- Programmazione delle attività

9.3.3 - Trattamento di dati personali effettuato con strumenti non elettronici

Premesso che i dati sono custoditi in appositi locali e classificatori il cui accesso è limitato al personale preposto, e non al pubblico, le misure adottate si limitano alla definizione d'incarichi ed istruzioni per il trattamento dei dati, e alla gestione degli stessi in modo selezionato e limitato agli usi necessari e permessi, per il periodo sufficiente al loro effettivo utilizzo. Infine non è previsto uno specifico impegno nella richiesta dell'utilizzo delle suddette informazioni, in quanto sono trattate ed utilizzate, solo ed esclusivamente per scopi attinenti l'esercizio dell'attività professionale dell'Istituto e mai, per scopi di diffusione o commerciali.

9.3.4 - Trattamento di dati sensibili effettuato con strumenti non elettronici

Oltre a quanto previsto al punto precedente, si è definito che i supporti fisici contenenti i dati siano tenuti sotto chiave, e che il loro accesso sia controllato. Queste misure si applicano anche ove siano detenute, a scopo d'archivio e/o protezione, copie cartacee di archivi gestiti elettronicamente dello stesso tipo.

9.4 - MISURE DI SICUREZZA ADOTTATE

Sono state adottate o scadenzate le seguenti misure di sicurezza:

9.4.1 - Organizzative

- Assegnazione d'incarichi,
- classificazione dei dati,
- verifiche sui trattamenti consentiti e/o corretti,
- analisi dei rischi,
- prescrizione di linee guida,
- formazione e sensibilizzazione del personale, in altre parole:
  - utilizzo delle password (Accesso, rete, screen saver), impostate sui personal computer,
  - variazione periodica delle password,
  - utilizzo corretto della posta elettronica (invio a più destinatari ed avvertenze per eventuali recapiti errati, risposta automatica ad uno /tutti i mittenti, copia conoscenza nascosta),
  - posizione del monitor nei confronti di eventuali persone esterne all'Istituto o altre categorie di incaricati,
  - conservazione dei documenti,
  - utilizzo corretto del retro delle fotocopie/fax,
  - utilizzo e riutilizzo corretto dei supporti magnetici (floppy disk),
  - organizzazione dei fax in ricezione,
  - corretto utilizzo del fax e sensibilizzazione sull'uso esatto del frontespizio,
  - gestione documenti contabili e relativi dati sensibili,
  - organizzazione della scrivania e gestione delle pratiche in affidamento,
  - corretto utilizzo e gestione delle chiavi degli armadi/cassetti contenenti dati personali.
- adeguamento formati per frontespizio fax in uscita,
- adeguamento delle procedure di gestione dei curriculum vitae ricevuti da vari canali, sia indotti sia spontanei.

9.4.2 - Fisiche

- Ingresso limitato e controllato nei locali ove avviene il trattamento,
- custodia dei dati cartacei in classificatori e/o armadi non accessibili.

9.4.3 - Logiche

- Controllo degli accessi ai computer, dati e/o ai programmi,
- costante controllo antivirus, sui dati e sulla posta elettronica,
- impostazione e configurazione ad accesso limitato degli screen saver,
- impostazione e configurazione di password per l'accesso di ogni computer.
- aggiunta automatica della firma di posta elettronica, contenente le avvertenze per il recapito errato dei messaggi.

9.5 - MISURE DI SICUREZZA DA ADOTTARE

9.5.1 - Organizzative

Nessuna, oltre a quelle già adottate.

9.5.2 - Fisiche

Nessuna, oltre a quelle già adottate.

9.5.3 - Logiche

Nessuna, oltre a quelle già adottate.

9.6 - STRUTTURA DELLA RETE

La struttura dei server di rete è identificata dalla seguente tabella.

Numero	Tipo	Sistema Operativo	Note
1	Server	Windows 2000 Server	Il sistema è utilizzato per il programma gestionale SISSI e per la gestione dei file office.

La struttura delle postazioni di rete Windows è identificata dalla seguente tabella.

Numero	Tipo	Sistema Operativo	Note
7	Desktop	Windows 8	I sistemi sono utilizzati per il programma gestionale SISSI e per la gestione dei file office. Una postazione della rete non è utilizzata per l'accesso al gestionale SISSI. Tutte le postazioni sono abilitate per l'accesso al portale ministeriale SIDI.
35	TABLET	-	Sono presenti in ogni classe utilizzate per i registri on line. Protetti da password.

La struttura per le connessioni di rete verso sedi remote e internet è riepilogata dalla seguente tabella.

Numero	Tipo	Note
1	ADSL	Utilizzate per i collegamenti ad internet non protetta da sistemi firewall hardware.

9.7 - MAPPA DEGLI APPLICATIVI

Nella tabella di seguito sono riportati gli applicativi installati presso la rete del titolare del trattamento.

Applicativo	*Descrizione*	*Produttore*	*Localizzazione*	*Outsourcer*
SIDI	Portale Ministeriale per la gestione del bilancio, gestione anagrafica alunni, personale docente e non docente.	Ministero della Pubblica Amministrazione	Server esterni	-
SISSI	Sistema utilizzato per la gestione del personale docente e non docente in materia di calcolo stipendi e certificati.	Ministero della Pubblica Amministrazione	Server interni con connessioni verso server esterni	-
Scuola Viva e Programma Alunni	Sistema viene utilizzato per il registro online presente in tutte le aule.		Server	-
Microsoft Office	Sistema di automazione di ufficio, utilizzato anche per la gestione della posta elettronica	Microsoft	PC locali	-

10 - INDICAZIONE DEGLI INDIRIZZI DI AGGIORNAMENTO

Al fine di mantenere le misure di sicurezza, per la riduzione del rischio, sono stati previsti i seguenti indirizzi di intervento:

- revisione annuale del presente documento programmatico per la sicurezza;
- aggiornamento giornaliero, direttamente dal sito internet del produttore, dei software antivirus, in concomitanza con la disponibilità degli stessi;
- aggiornamento periodico delle password di sistema;
- verifica, manutenzione e gestione degli archivi cartacei e magnetici.

11 - CONSERVAZIONE

In conformità a quanto previsto dal D.Lgs. 196/2003, il presente documento, sarà conservato a cura del titolare del trattamento, presso la sede dell'Istituto.

12 - APPROVAZIONE DEL DOCUMENTO

Titolare del trattamento.

Il legale rappresentante	*Firma*
PROF.SSA ELENA MARGHERITA	

Responsabile del trattamento.

Cognome nome	*Firma*
Adriana Dentella	

Vertova,

Data
5 GIUGNO 2017