



*Ministero dell'Istruzione, dell'Università e della Ricerca*

*Ufficio Scolastico Regionale per il Veneto*

**SCUOLA SECONDARIA PRIMO GRADO "A. GIURIOLO"**

**CENTRO TERRITORIALE PERMANENTE-ISTRUZIONE IN ETÀ ADULTA (CTP-EDA)**

Cod.Fisc 81001350248 Cod Mecc. VIMM11100B E-Mail smsarzignano@libero.it  
via IV Martiri, 71 – 36071 ARZIGNANO (VI) – Tel. 0444/670400 - fax: 0444/671495

# DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

D.Lgs. N° 196 del 30/06/2003

Data emissione	31 marzo 2011
Periodo validità	anno 2011
Firma titolare del Trattamento	dott.ssa Donata Albiero
Prot. n.	_Prot. 1785/A07

**DEPOSITO ATTI 31/03/2011, PROT 1785/A07**



## Modifiche e integrazioni

Anno	Rev.	Par.	Descrizione
2008	2	1	Aggiornati i riferimenti al D.M. n° 305 del 7/12/2006
		All.	Aggiornata la pianta degli archivi ed i responsabili
	1_1	-	Aggiornato l'elenco allegati
		-	Aggiornato lo schema di sistema informatico
		2	Aggiornata tabella 1 con i nominativi delle strutture preposte al trattamento
2009	4	4	ANALISI DEI RISCHI: Aggiornata tabella 4: modificato rischio collegato al comportamento operatori per "Carenza di consapevolezza, disattenzione o incuria, eccesso di diffusione dei dati"
		3	Aggiornata l'analisi dei rischi: aggiornata la tabella con valori di rischio e abbassamento del rischio generale
2010	4	1.3	Aggiornate le finalità con il decreto ministeriale
		2	Introdotta organigramma per incarichi Tab1
		4	Aggiornata analisi dei rischi
2011	5	4	Aggiornata analisi dei rischi

### Sommario

1	ELENCO DEI TRATTAMENTI E DEI DATI PERSONALI DI NATURA COMUNE O SENSIBILE .....	4
1.1	Informazioni generali .....	4
1.2	Termini e definizioni .....	4
1.3	Finalità: .....	5
1.4	Fonte dei dati: .....	5
1.5	Tipologia dei dati .....	6
2	DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA' NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI. 7	
3	AMBITO DEI TRATTAMENTI.....	8
4	ANALISI DEI RISCHI INCOMBENTI SUI DATI. ....	10
5	MISURE ADOTTATE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI, NONCHE' LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITA'. ....	13
6	CRITERI E DELLE MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO.....	15
7	PROGRAMMA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO. ....	17
8	TRATTAMENTI DI DATI PERSONALI SENSIBILI O GIUDIZIARI CON STRUMENTI ELETTRONICI AFFIDATI ALL'ESTERNO. ....	18
8.1	VINCOLI CONTRATTUALMENTE ASSUNTI DAL FORNITORE ESTERNO AI FINI DELLA SICUREZZA DEI DATI. ....	18
9	ATTI E DOCUMENTI NON IN FORMATO ELETTRONICO, ARCHIVI CARTACEI. ....	19
10	OBBLIGO DI AGGIORNAMENTO PERIODICO. ....	20

### Sommario Tabelle

Tabella 1:	organigramma per incarichi .....	7
Tabella 2:	Elenco dei trattamenti: informazioni di base .....	8
Tabella 3:	Elenco dei trattamenti: descrizione degli strumenti utilizzati .....	8
Tabella 4:	Analisi dei rischi .....	10
Tabella 5:	Le misure di sicurezza adottate .....	13
Tabella 6:	Procedure di copia, verifica e ripristino per ogni singola unità contenente dati .....	15



<i>Tabella 7: Ripristino dei dati</i> .....	16
<i>Tabella 8: Elenco adempimenti</i> .....	20

### **Elenco Allegati**

*Allegato 1:Regolamento per la gestione dei dati personali e sensibili.*

*Allegato 1/1:Pianta gestione archivi*

*Allegato 2:Regolamento informatico*

*Allegato 3:Nomina a Responsabile del trattamento.*

*Allegato 4:Incarichi al trattamento*

*Allegato 5:Nomina Responsabile del trattamento Amministratore di sistema.*

*Allegato 6:Nomina Responsabile del trattamento Ente esterno.*

*Allegato 7:Lettere di rispetto.*



# 1 ELENCO DEI TRATTAMENTI E DEI DATI PERSONALI DI NATURA COMUNE O SENSIBILE

## 1.1 Informazioni generali

Le informazioni riguardanti i dati personali, sensibili e giudiziari trattati all'interno dell'istituto circa:

- Tipologie di trattamento e contesto;
- Finalità di interesse pubblico perseguite
- Fonti normative;
- Tipologia di dati trattati;
- Operazioni eseguite;

sono riportate in modo specifico all'interno del D.M. n° 305 del 7/12/2006. in questo documento sono riportate in modo riassuntivo e non esaustivo.

## 1.2 Termini e definizioni

Ai fini del presente documento, si applicano le definizioni di cui all'art. 4 del D.lg. 196/2003, che riportiamo in parte per comodità:

a) **"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;

b) **"dati identificativi"**, i dati personali che permettono l'identificazione diretta dell'interessato;

c) **"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;

d) **"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;

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

f) **"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;

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

h) **"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;

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

l) **"trasferimento all'estero"**, il trasferimento dei dati personali aziendali fuori dal territorio dell'UE, con qualunque mezzo o sistema effettuato, quale, a mero titolo di esempio, l'invio tramite e-mail di liste e/o elenchi di interessati con o senza ulteriori informazioni; il trasporto di liste e/o elenchi di Interessati con o senza ulteriori informazioni tramite personal computer portatile, floppy disk, CD Rom, o altri idonei supporti; l'inoltro di fax, lettere o altri documenti cartacei contenenti liste e/o elenchi di Interessati con o senza ulteriori informazioni;

Inoltre, valgono le definizioni delle seguenti figure o funzioni appartenenti al modello organizzativo privacy:

a) **"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;

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

c) **"amministratori di sistema"**, i soggetti cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di basi di dati e di consentirne l'utilizzazione (ovvero, alcuni Incaricati dell'UO Sistemi informativi, autorizzati all'uso delle password di "administrator" dei sistemi operativi o applicativi);

d) **"gestori delle password"**, i soggetti cui è conferito il compito di custodire le password utilizzate in azienda o accedere alle informazioni ad esse relative e gestire le relative procedure (ovvero, alcuni Incaricati dell'UO Sistemi informativi, autorizzati all'uso delle password di "administrator" dei sistemi operativi o applicativi);



e) **"incaricati"**, le persone fisiche autorizzate a compiere operazioni di trattamento (vedi "trattamento") dal titolare o dal responsabile, (ovvero, tutto il personale che abbia accesso a dati personali e, in quanto tale, individuato per iscritto come incaricato da parte del responsabile del trattamento competente per l'UO di riferimento);

f) **"incaricati autorizzati"**, il personale che effettua operazioni di trattamento (vedi "trattamento") di dati sensibili in relazione alle proprie mansioni lavorative (ovvero, tutto il personale che abbia accesso a dati sensibili e, in quanto tale, autorizzato a livello di area di appartenenza da parte del responsabile delegato privacy e/o dal responsabile del trattamento competente per l'UO di riferimento)

g) **"incaricati della manutenzione"**, le persone fisiche autorizzate, dal titolare o dal responsabile, a compiere operazioni di trattamento in relazione a mansioni inerenti la gestione o manutenzione dei sistemi hardware e software;

i) **"interessato"**, la persona fisica, la persona giuridica, l'ente o l'associazione cui si riferiscono i dati personali (per esempio: clienti, fornitori, dipendenti, candidati, ecc.);

Infine, si intende per:

a) **"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 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;

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

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

d) **"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;

e) **"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;

f) **"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;

g) **"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.

### 1.3 Finalità:

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

1. Selezione e reclutamento a tempo indeterminato e determinato e gestione del rapporto di lavoro;
2. Gestione del contenzioso e provvedimenti disciplinari;
3. Organismi collegiali e istituzionali;
4. Attività propedeutiche all'avvio dell'anno scolastico;
5. Attività educativa, didattica, formativa e di valutazione;
6. Scuole non statali (NON APPLICABILE)
7. Rapporti scuola-famiglia: gestione del contenzioso.

### 1.4 Fonte dei dati:

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

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



Un regolamento ministeriale specifico disciplina il trattamento dei dati personali nella scuola secondaria di primo grado Antonio Giuriolo in attuazione di quanto disposto dal D.L. 196/2003 (allegato n. 1).

Un regolamento specifico, disciplina la gestione del sistema informatico (allegato n. 2)

### **1.5 Tipologia dei dati**

Sulla scorta delle precisazioni indicate nel D.M. n° 305 del 7/12/2006, l'istituzione scolastica, sulla base di una prima ricognizione, fatta salva la possibilità di procedere a successive integrazioni e/o correzioni entro le scadenze previste dalla legge, dichiara, con riferimento ai destinatari o famigliari dei destinatari dell'offerta formativa ovvero del personale coinvolto, a qualunque titolo, nella medesima, o interessato ad essere coinvolto, ovvero di soggetti, a qualsiasi titolo, coinvolti in rapporti negoziali con l'istituzione scolastica, o aspiranti ad assumere tale ruolo, di trattare i dati di seguito elencati:

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



## 2 DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITÀ NELL'AMBITO DELLE STRUTTURE PREPOSTE AL TRATTAMENTO DEI DATI.

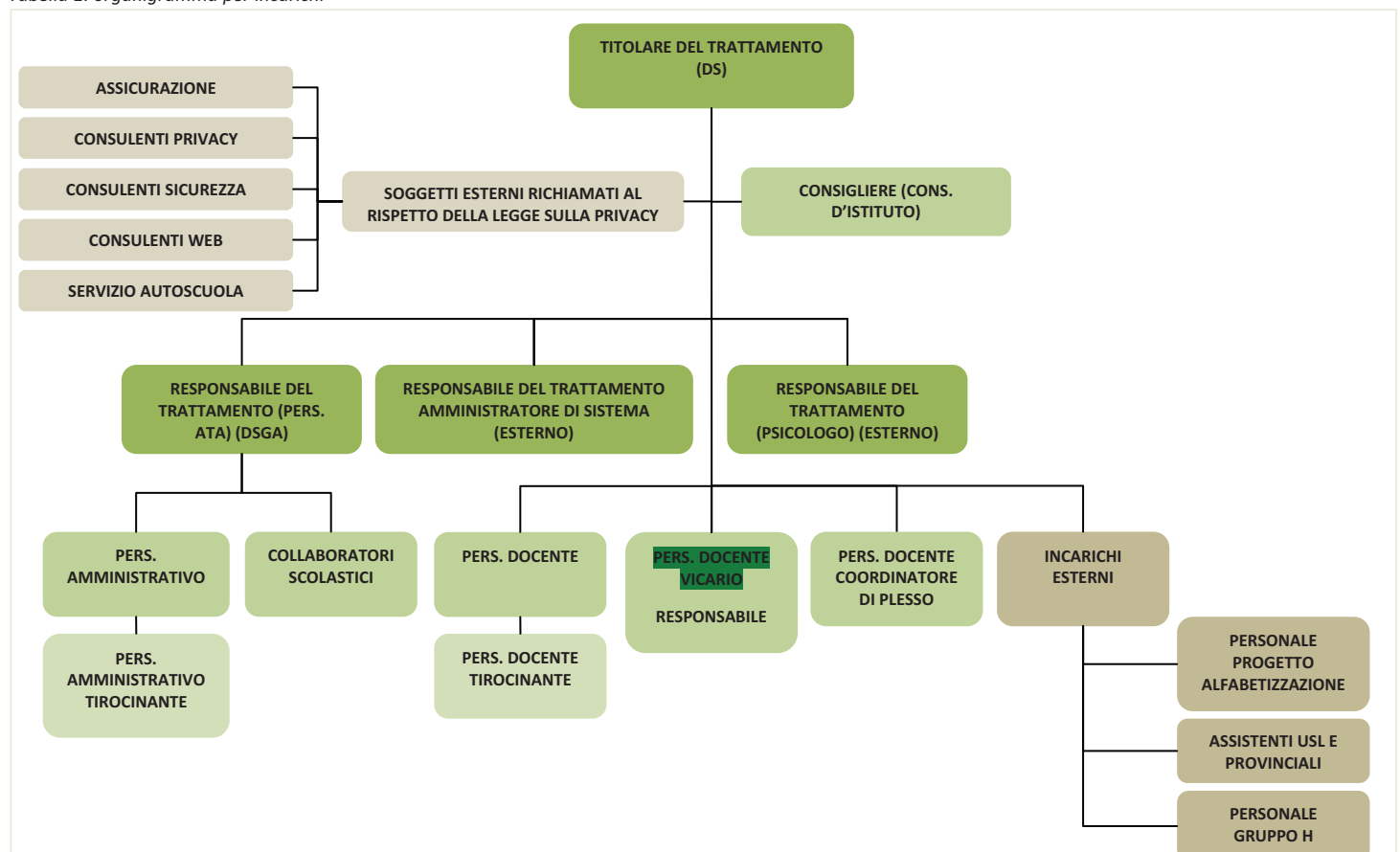
L'ente titolare del trattamento dei dati ha designato il Responsabile ai sensi dell'art. 29 del D. Lgs. N° 196 del 2003 e gli incaricati ai sensi dell'art. 30 del D. Lgs. N° 196 del 2003.

In particolare:

- l'ambito dei trattamenti autorizzati ai singoli incaricati è suscettibile di aggiornamento periodico come da normativa;
- a tutti gli incaricati destinati al trattamento di dati mediante strumento elettronico, sono state conferite credenziali di autenticazioni (art. 34, comma 1, lett. b) mediante parola chiave, conformi alle caratteristiche indicate nell'allegato B;
- il DSGA responsabile del trattamento dati, conserva nella cassaforte dell'ufficio di presidenza copie delle credenziali come da atto di consegna;
- le suddette credenziali sono disattivate automaticamente dal gestore della rete (Amministratore di sistema) periodicamente, ovvero in tutti i casi di mancata utilizzazione per almeno 6 mesi;
- concorre al trattamento anche una struttura esterna all'istituzione scolastica, incaricata mediante nomina di responsabile trattamento dati come AMMINISTRATORE DI SISTEMA (allegato n. 5);
- il titolare della struttura incaricata è stato designato quale responsabile del trattamento, in ragione del contratto di manutenzione stipulato con questa Istituzione Scolastica e per tutto il tempo della sua durata;
- il titolare ha anche nominato, quale responsabile del trattamento dati alunni del CTP, il rappresentante legale Ente esterno che svolge attività di prestazione d'opera (allegato n. 6);

nel complesso i contenuti delle nomine sono definiti nelle lettere di incarico mentre il quadro completo delle nomine è definito dal seguente organigramma per incarichi:

Tabella 1: organigramma per incarichi





### 3 AMBITO DEI TRATTAMENTI.

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

Tabella 2: Elenco dei trattamenti: informazioni di base

Struttura deputata al trattamento	Natura dei dati trattati	Struttura di riferimento	Altre strutture (anche esterne) che concorrono al trattamento	Descrizione degli strumenti utilizzati
Ufficio Dirigente Scolastico	<input checked="" type="checkbox"/> Sensibili <input checked="" type="checkbox"/> Giudiziali	Sede Istituzione Scolastica	Ditta esterna amministratore di sistema, limitatamente alle esigenze di manutenzione e/o riparazione dei PC interni e/o del server	PC interni + server
Ufficio Direttore dei Servizi				PC interno + server sito in ufficio di segreteria (personale)
Ufficio Personale;				PC interni + server
Servizi inerenti l'offerta formativa;				PC interni + server
Servizi strumentali agli organi collegiali;				PC interni + server
Ufficio CTP				PC interno + server sito in ufficio di segreteria (personale)

Il trattamento dei dati avviene attraverso modalità diverse: strumenti elettronici collegati in rete fra loro e alla rete internet.

Con riferimento alla gestione dei dati mediante rete ministeriale, l'istituzione scolastica declina ogni responsabilità, operando come semplice utente non essendo in grado di intervenire sulla gestione delle informazioni ivi contenute e gestite.

Con riferimento all'ubicazione fisica dei supporti di memorizzazione delle copie di sicurezza, l'Istituzione scolastica, tenendo conto dell'analisi di cui al punto 5, ha ritenuto di provvedere alla custodia presso la cassaforte nell'ufficio del dirigente.

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

Tabella 3: Elenco dei trattamenti: descrizione degli strumenti utilizzati

IDENTIFICATIVO DEL TRATTAMENTO	EVENTUALE BANCHE DATI DI SUPPORTO	UBICAZIONE FISICA DEI SUPPORTI DI MEMORIZZAZIONE E DELLE COPIE DI SICUREZZA	TIPOLOGIA DI DISPOSITIVI DI ACCESSO	TIPOLOGIA DI INTERCONNESSIONE
1. Selezione e reclutamento a tempo indeterminato e determinato e gestione del rapporto di lavoro;	Database file office	Nei locali dell'Istituzione scolastica siti al Piano Terra presso la sede e i plessi	PC	Rete locale e Internet
2. Gestione del contenzioso e provvedimenti disciplinari;	Database file office			
3. Organismi collegiali e istituzionali;	Database file office			
4. Attività propedeutiche all'avvio dell'anno scolastico;	Database file office			
5. Attività educativa, didattica, formativa e di valutazione;	Database gestionale Database file office			
6. Scuole non statali (NON				

**SCUOLA SECONDARIA PRIMO GRADO "A. GIURIOLO"**

CENTRO TERRITORIALE PERMANENTE-ISTRUZIONE IN ETÀ ADULTA (CTP-EDA)

Rev. 05 del 01/03/2011

**Documento Programmatico della Sicurezza (DPS)**

IDENTIFICATIVO DEL TRATTAMENTO	EVENTUALE BANCHE DATI DI SUPPORTO	UBICAZIONE FISICA DEI SUPPORTI DI MEMORIZZAZIONE E DELLE COPIE DI SICUREZZA	TIPOLOGIA DI DISPOSITIVI DI ACCESSO	TIPOLOGIA DI INTERCONNESSIONE
<b>APPLICABILE</b>				
7. Rapporti scuola-famiglia: gestione del contenzioso.				



## 4 ANALISI DEI RISCHI INCOMBENTI SUI DATI.

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

Le fonti di rischio sono state accorpate in:

### 1) Comportamenti degli operatori.

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

### 2) Eventi relativi agli strumenti.

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

### 3) Eventi relativi al contesto fisico-ambientale.

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

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

Tabella 4: Analisi dei rischi

#### IMPATTO SULLA SICUREZZA DEI DATI

EVENTO	Descrizione	Gravità Stimata	VALORE	RIF. MISURE DI AZIONE	
Comportamenti degli operatori	Furto di credenziali di consapevolezza, disattenzione o incuria	M	7	Vigilanza sul rispetto delle istruzioni impartite	
	Carenza di consapevolezza, disattenzione o incuria, eccesso di diffusione dei dati	MA	8	Formazione e flusso continuo di informazione	
	Comportamenti sleali o fraudolenti	Dispersione, perdita e accesso altrui non autorizzato	B	5	Vigilanza sul rispetto delle istruzioni impartite
	Errore materiale	Dispersione, perdita e accesso altrui non autorizzato	MA	8	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
	Azione di virus informatici o di codici malefici	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaborati	MA	8	Adozione di idonei dispositivi di protezione
Eventi relativi agli strumenti	Spamming o altre tecniche di sabotaggio	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	8	Adozione di idonei dispositivi di protezione



**Documento Programmatico della Sicurezza (DPS)**

	Malfunzionamento, indisponibilità o degrado degli strumenti	Perdita o alterazione, anche irreversibile, di dati, di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	8	Assistenza e manutenzione continua degli elaboratori e dei programmi; ricambio periodico
	Accessi esterni non autorizzati	Dispersione, perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	8	Adozione di idonei dispositivi di protezione
	Intercettazione di informazioni in rete	Dispersione di dati; accesso altrui non autorizzato	MA	8	Adozione di idonei dispositivi di protezione
Eventi relativi al contesto	Accessi non autorizzati a locali/reparti ad accesso ristretto	Dispersione perdita o alterazione, anche irreversibile, di dati, nonché manomissione di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	8	Protezione dei locali mediante serratura con distribuzione delle chiavi ai soli autorizzati sia da parte della scuola <b>(allegato n.7)</b> sia da parte degli Enti locali per quanto di competenza <b>(allegato n. 7/1)</b>
	Asportazione e furto di strumenti contenenti dati	Dispersione e perdita di dati, di programmi e di elaboratori; accesso altrui non autorizzato	MA	8	Protezione dei locali e dei siti di ubicazioni degli elaboratori e dei supporti di memorizzazione mediante serratura con distribuzione delle chiavi ai soli autorizzati
	Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria	Perdita di dati, dei programmi e degli elaboratori	MB	6	Attività di prevenzione, controllo, assistenza e manutenzione periodica, vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, etc.)	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaboratori; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	8	Attività di controllo, assistenza e manutenzione periodica
	Errori umani nella gestione della sicurezza fisica	Perdita o alterazione, anche irreversibile, di dati, nonché manomissione dei programmi e degli elaborati; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	MA	8	Vigilanza sul rispetto delle istruzioni impartite, formazione e flusso continuo di informazione
<b>TOTALE</b>				<b>7,57</b>	

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

**A**=alto 10

**EE**=molto elevato 9

**M**=medio 7

**MA**=medio-alto 8



**SCUOLA SECONDARIA PRIMO GRADO "A. GIURIOLO"**

CENTRO TERRITORIALE PERMANENTE-ISTRUZIONE IN ETÀ ADULTA (CTP-EDA)

**Documento Programmatico della Sicurezza (DPS)**

Rev. 05 del 01/03/2011

**MB**=medio-basso 6

**B**=basso 5



## 5 MISURE ADOTTATE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI, NONCHE' LA PROTEZIONE DELLE AREE E DEI LOCALI, RILEVANTI AI FINI DELLA LORO CUSTODIA E ACCESSIBILITA'.

Sulla scorta della ricognizione dei rischi sopra rappresentata, l'istituzione scolastica ha provveduto ad apprestare e/o introdurre strumenti di tutela, ovvero a prevedere successive, e più incisive, misure di sicurezza.

La tabella seguente sintetizza le misure di sicurezza in essere, corredate da indicazioni di dettaglio.

Tabella 5: Le misure di sicurezza adottate

RISCHIO CONTRASTATO	MISURA	STRUTTURA INTERESSATA	EVENTUALE BANCA DATI INTERESSATA	MISURA GIA' IN ESSERE	PERIODICITA' E RESPONSABILITA' DEI CONTROLLI
Dispersione, perdita o alterazione anche irreversibile, di programmi e di elaboratori; accesso altrui non autorizzato; impossibilità temporanea di accesso ai dati e di utilizzo dei programmi	Preventiva, di contrasto, di contenimento degli effetti	Ufficio Dirigente Scolastico	Relativo archivio	Antivirus, Firewall e Password	Bimestrale; responsabile pro tempore del servizio (ditta LSK di Cervato Massimo)
Come sopra	Preventiva, di contrasto, di contenimento degli effetti	Ufficio DSGA	Relativo archivio	Antivirus, Firewall e Password	Bimestrale; responsabile pro tempore del servizio (ditta LSK di Cervato Massimo)
Come sopra	Preventiva, di contrasto, di contenimento degli effetti	Ufficio Personale Servizi inerenti l'offerta formativa Servizi strumentali agli organi collegiali	Relativo archivio	Antivirus, Firewall e Password	Bimestrale; responsabile pro tempore del servizio (ditta LSK di Cervato Massimo)
Come sopra	Preventiva, di contrasto, di contenimento degli effetti	Ufficio CTP	Relativo archivio	Antivirus, Firewall e Password	Bimestrale; responsabile pro tempore del servizio (ditta LSK di Cervato Massimo)

Specificatamente, le misure di sicurezza di carattere elettronico/informatico adottate sono:

- utilizzo di server con configurazioni di ridondanza attiva in doppio livello di ridondanza (doppio HD sul server + BACK UP)
- presenza di gruppi di continuità elettrica per il server;
- è attivo un sistema di back-up centralizzato e automatizzato con periodicità giornaliera e storico mensile. Alla data di questo documento il responsabili delle copie è l'amministratore di sistema;
- è attivo un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso Internet;
- è attivo un sistema di definizione delle regole per la gestione delle password per i sistemi operativi windows 2000 e XP di seguito specificati.

In particolare le periferiche atte a preservare una sicurezza contro intrusioni esterne verso i computer della segreteria sono:

- **Router Cisco SOHO 76 con Firewall** – L'apparato non è stato installato dalla ditta LSK di Cervato Massimo, quindi non è accessibile per controllare eventuali configurazioni. Il router è posto in un armadietto rack a muro in aula informatica alunni.



- **Server Segreteria** – Il server gestisce lo smistamento della connessione internet proveniente dall'ultimo piano in aula informatica. Nel server sono installate due schede di rete con indirizzi IP in classe diversa. La prima scheda di rete riceve dati direttamente dal router, e li passa alla seconda scheda di rete, che, collegata ad un hub, smista la connessione al resto dei computer in segreteria. Anche in questo caso l'hub che dal server parte verso le diverse postazioni risiede in un armadio rack a parete in segreteria.



## 6 CRITERI E DELLE MODALITA' PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI IN SEGUITO A DISTRUZIONE O DANNEGGIAMENTO.

Al fine di garantire l'integrità dei dati contro i rischi di distribuzione o perdita, è stata definita una procedura di periodica esecuzione di copie di sicurezza dei dati trattati. Sono state perciò acquisite licenze di uso per software antivirus, nonché sistemi di firewall con verifica di idoneità e costante aggiornamento. In ogni caso si osserva che l'istituzione scolastica dispone di un sistema di controllo degli accessi ai locali, di un sistema di allarme e videocitofono per l'ingresso ( predisposti dal Comune di Arzignano)

I documenti sono anche in copia cartacea presso locali dell'istituzione scolastica non accessibili ai terzi e dotati di adeguati strumenti di protezione (armadi con serrature, stanze protette da inferriate).

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

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

Struttura in possesso di PC o collegamento a server	Applicativo	Sistema operativo	Supporti magnetici	Procedura di copia	Procedura di verifica	Ripristino
Ufficio Dirigente Scolastico	Office	Server Windows XP professional	Cassette Tipo DAT	Procedura di back-up Windows 2000 sever	Procedura di back-up Windows 2000 server	Procedura di back-up Windows 2000 server
Ufficio DSGA		Server Windows 2000 professional				
Ufficio Personale		Server Windows 2000 professional				
Servizi inerenti l'offerta formativa		Server Windows 2000 e Windows XP professional				
Servizi strumentali agli organi collegiali		Server Windows 2000 professional				
Ufficio CTP		Server Windows XP professional				

Con riferimento invece al contenuto ed alle competenze in tema di copia, verifica e ripristino, le soluzioni organizzative adottate presso l'istituzione scolastica sono sintetizzate nella seguente tabella n 7 e descritte nelle ISTRUZIONI OPERATIVE BACKUP E RIPRISTINO.

Tabella 7 Salvataggio dei dati

SALVATAGGIO		CRITERI INDIVIDUATI PER IL SALVATAGGIO	UBICAZIONE DI CONSERVAZIONE DELLE COPIE	STRUTTURA OPERATIVA INCARICATA DEL SALVATAGGIO
STRUTTURA	DATI SENSIBILI O GIUDIZIARI CONTENUTI			
Ufficio Dirigente Scolastico		Salvataggio dati periodico: <ul style="list-style-type: none"> <li>Giornaliero automatico fatto dal server su DAT</li> </ul>	Cassaforte sita nell'Ufficio D SGA con serratura chiavi distribuite fra i soli autorizzati. L'ufficio sito al piano terra, con accesso dall'esterno e dal corridoio, con serratura con chiavi distribuite fra i soli autorizzati.	Responsabile pro tempore del servizio  (ditta LSK di Cervato Massimo)
Ufficio D SGA	Dati giudiziari inerenti imprese interessate ad attività negoziali	Salvataggio dati periodico: <ul style="list-style-type: none"> <li>Giornaliero automatico fatto dal server su DAT</li> </ul>	Cassaforte sita nell'Ufficio D SGA con serratura chiavi distribuite fra i soli autorizzati. L'ufficio sito al piano terra, con accesso dall'esterno e dal corridoio, con serratura con chiavi distribuite fra i soli	

**SCUOLA SECONDARIA PRIMO GRADO "A. GIURIOLO"**

CENTRO TERRITORIALE PERMANENTE-ISTRUZIONE IN ETÀ ADULTA (CTP-EDA)

Rev. 05 del 01/03/2011

**Documento Programmatico della Sicurezza (DPS)**

SALVATAGGIO		CRITERI INDIVIDUATI PER IL SALVATAGGIO	UBICAZIONE DI CONSERVAZIONE DELLE COPIE	STRUTTURA OPERATIVA INCARICATA DEL SALVATAGGIO
STRUTTURA	DATI SENSIBILI O GIUDIZIARI CONTENUTI			
			autorizzati.	
Ufficio Personale	<ul style="list-style-type: none"> <li>Stato di salute (assenze di varia natura);</li> <li>Adesione a sindacati;</li> <li>Origine razziale o etnica;</li> <li>Confessione religiosa;</li> <li>Stato di salute;</li> </ul>	Salvataggio dati periodico: <ul style="list-style-type: none"> <li>Giornaliero automatico fatto dal server su DAT</li> </ul>	Cassaforte sita nell'Ufficio DSGA con serratura chiavi distribuite fra i soli autorizzati. L'ufficio sito al piano terra, con accesso dall'esterno e dal corridoio, con serratura con chiavi distribuite fra i soli autorizzati.	
Servizi inerenti l'offerta formativa	<ul style="list-style-type: none"> <li>Origine razziale o etnica;</li> <li>Confessione religiosa;</li> </ul>			
Servizi strumentali agli organi collegiali	<ul style="list-style-type: none"> <li>Origine razziale o etnica;</li> <li>Confessione religiosa;</li> </ul>			
Ufficio CTP	<ul style="list-style-type: none"> <li>Stato di salute;</li> <li>Origine razziale o etnica;</li> <li>Confessione religiosa;</li> </ul>	Salvataggio dati periodico: <ul style="list-style-type: none"> <li>Giornaliero automatico fatto dal server su DAT</li> </ul>	Cassaforte sita nell'Ufficio DSGA con serratura chiavi distribuite fra i soli autorizzati. L'ufficio sito al piano terra, con accesso dall'esterno e dal corridoio, con serratura con chiavi distribuite fra i soli autorizzati.	

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

Tabella 7: Ripristino dei dati

DATA BASE/ARCHIVIO	SCHEDA OPERATIVA	PIANIFICAZIONE DELLE PROVE DI RIPRISTINO
Segreteria Dirigente Scolastico	Viene effettuato un back-up dei dati trattati e dei documenti presenti sull'HD su diverse copie di supporti che vengono conservate in più locali con serratura, ma sempre all'interno della sede dell'istituzione scolastica della Scuola Secondaria di Primo Grado "A. Giuriolo" - Arzignano (VI)	Trimestrale
Ufficio Direttore dei Servizi Amministrativi	Come sopra	Trimestrale
<ul style="list-style-type: none"> <li>Ufficio Personale;</li> <li>Servizi inerenti l'offerta formativa;</li> <li>Servizi strumentali agli organi collegiali;</li> </ul>	Come sopra	Trimestrale
Ufficio CTP	Come sopra	Trimestrale



## **7 PROGRAMMA DEGLI INTERVENTI FORMATIVI DEGLI INCARICATI DEL TRATTAMENTO.**

L'istituzione scolastica intende aderire alle iniziative formative organizzate dalla direzione regionale del Ministero dell'Istruzione dell'Università e della Ricerca Scientifica, tenendo anche conto dell'economicità di un'azione organizzata su base regionale, rispetto ad una gestione in proprio delle attività formative.

L'Istituzione opera integrale rinvio alla programmazione della Direzione regionale, riservandosi in ogni caso di agire in via suppletiva, qualora, per ragione organizzative od economiche, non è possibile far partecipare il proprio personale alle attività di formazione necessarie per adempiere alle prescrizioni ordinamentali.

Gli interventi formativi nei confronti degli incaricati del trattamento vengono fatti periodicamente attraverso **riunioni interne e corsi di formazione esterni**, ed hanno l'obiettivo di renderli edotti:

1. dei rischi che incombono sui dati;
2. delle misure disponibili per prevenire eventi dannosi
3. dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività;
4. delle responsabilità che ne derivano;
5. 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.

In particolare il Titolare del trattamento effettua almeno una riunione formativa all'anno sulla privacy e ne redige **apposito verbale** da conservare negli archivi dell'Amministrazione dell'Istituto



## **8 TRATTAMENTI DI DATI PERSONALI SENSIBILI O GIUDIZIARI CON STRUMENTI ELETTRONICI AFFIDATI ALL'ESTERNO.**

L'Istituzione scolastica, ha proceduto all'esternalizzazione di taluni trattamenti, secondo modalità conformi a quanto previsto dal D.Lgs. n° 196 del 2003, procedendo alla nomina di un soggetto esterno quale responsabile del trattamento, limitatamente ai dati e alle operazioni necessarie per lo svolgimento delle attività conferite.

A tal fine l'Istituzione scolastica ha imposto le cautele indicate in calce alla tabella che segue, affinché il soggetto destinatario adotti le misure di sicurezza richieste dal Codice, ivi incluso il relativo all. B.

Per i soggetti indicati nell'organigramma per incarichi, l'atto di nomina è allegato al presente DPS e definisce gli ambiti del trattamento.

### **8.1 VINCOLI CONTRATTUALMENTE ASSUNTI DAL FORNITORE ESTERNO AI FINI DELLA SICUREZZA DEI DATI.**

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

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



## **9 ATTI E DOCUMENTI NON IN FORMATO ELETTRONICO, ARCHIVI CARTACEI.**

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

Tutti i documenti contenenti dati sensibili sono conservati rigorosamente in buste chiuse e custodite all'interno di armadi chiusi a chiavi.

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



## 10 OBBLIGO DI AGGIORNAMENTO PERIODICO.

Elenco dei principali adempimenti formali minimi necessari alla corretta gestione del sistema di protezione dei dati personali e sensibili.

*Tabella 8: Elenco adempimenti*

<b>Adempimento</b>	<b>Cadenza ordinaria/consigliata</b>	<b>Scadenza</b>
1. Analisi dei rischi	Almeno 1 volta all'anno	31/03 di ogni anno
2. Verifica misure stabilite	Almeno 1 volta all'anno	31/03 di ogni anno
3. Verifica sistema autorizzativo	Almeno 1 volta all'anno	31/03 di ogni anno
4. Verifica sistema Informatico	Almeno 1 volta all'anno	31/03 di ogni anno
5. Formazione del personale incaricato	Almeno 1 volta all'anno	31/03 di ogni anno
6. Prova di ripristino dei dati	Almeno 1 volta all'anno	31/03 di ogni anno
7. Rimissione con data certa del DPS	Almeno 1 volta all'anno	31/03 di ogni anno

Note in allegato

Pianta gestione archivi aggiornata 31 Marzo 2011 Prot. 1785/A07

Delibera consiglio di istituto su aggiornamento DPS 31 marzo 2011