ISTRUZIONE MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
ISTITUTO COMPRENSIVO STATALE SAN PAOLO D'ARGON
Via Convento, 29 –24060 San Paolo d'argon (Bg)
Tel: 035 958054– Fax: 035959618
Sito: www.icsanpaolodargoncenatesotto.gov.it
Posta Certificata: bgic870003@pec.istruzione.it
c.f. 95119200160

DOCUMENTO PROGRAMMATICO

SULLA SICUREZZA

DISCIPLINARE TECNICO 2015

DIRIGENTE SCOLASTICO - PROF.VINCENZO DEMICHELE -

PROTOCOLLO -

DELIBERA DEL CONSIGLIO DI ISTITUTO I .N. DEL

STATO DOCUMENTO – DEFINITIVO-

DATA CREAZIONE -01/09/2014-

DATA ULTIMO AGGIORNAMENTO FEBBRAIO 2015
RESPONSABILI

DIRIGENTE SCOLASTICO

DIRETTORE DEI SERVIZI GENERALI E AMMINISTRATIVI

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA - 2015

Premessa

L'ISTITUTO COMPRENSIVO STATALE di San Paolo d'Argon, con sede in via Locatelli n. 3, SAN PAOLO D'ARGON – BG – C.F. 95119200160. nella persona del suo legale rappresentante Dirigente Scolastico Prof. Vincenzo Demichele, ha redatto il seguente DISCIPLINARE TECNICO per la Sicurezza pur essendo entrato in vigore il DL n. 5/2012, meglio conosciuto come DL semplificazioni, per effetto della pubblicazione sulla GU n. 33 del 9/2/2012. Tra le "semplificazioni"più rilevanti figurano quelle relative ai dati personali. In particolare, l'art.45 del DL semplificazioni interviene sull'art. 34 del Codice della privacy (Dlgs. 196/2003), sopprimendo la lett. G) del comma 1 e abrogato il comma 1-bis.

Sebbene il DL n. 5/2012, abbia reso non più obbligatorio la tenuta di un DPS aggiornato e della necessità di avvalersi di un'autocertificazione sostitutiva o di un DPS semplificato per i soggetti che trattano unicamente dati personali non sensibili e, come solo dati sensibili, trattano quelli dei propri dipendenti e collaboratori, inclusi coniuge e si è ritenuta necessaria la predisposizione e l'aggiornamento dei dati 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. Tale abolizione, comunque, lascia inalterato l'obbligo dell'istituzione delle misure di sicurezza per la tutela dei dati sensibili. Nonostante tale abrogazione sono rimasti invariati tutti gli aspetti tecnici della normativa:

1. autenticazione informatica
2. adozione di procedure di gestione delle credenziali di autenticazione
3. utilizzazione di un sistema di autorizzazione
4. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici
5. protezione degli strumenti elettronici e dei dati rispetto a trattamenti illeciti di dati, ad accessi non consentiti e a determinati programmi informatici
6. adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi
7. adozioni di tecniche di cifratura o di codici identificativi per determinati trattamenti di dati idonei a rivelare lo stato di salute o la vita sessuale effettuati da organismi sanitari

Rimane, pertanto, la necessità di stilare:

- l'elenco dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché le procedure da seguire per controllare l'accesso ai locali nei quali vengono conservati i dati oggetto del trattamento o l'accesso per via telematica;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento garantendone la disponibilità in tempi certi compatibili con i diritti degli interessati;

- la previsione di interventi formativi per rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati e dei modi per prevenire i danni delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare o sull'introduzione di nuovi strumenti utilizzati per il trattamento dei dati personali;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rivelare lo stato di salute e la vita sessuale, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Con il presente disciplinare, si disegna il quadro delle misure di sicurezza, organizzative, fisiche e logistiche, che sono adottate dall'Istituto Comprensivo di Terno sul trattamento dei dati personali, per le rispettive competenze, da parte del DSGA, degli Assistenti Amministrativi, del personale Docente e di Collaboratori Scolastici per le finalità istituzionali della scuola, che sono quelle concernenti l'istruzione e alla formazione degli alunni e quelle amministrative ad esse strumentali, cosi come definite dalla normativa vigente.

2.1. Riferimenti normativi

- Legge 31/12/1996 n. 675 e successive modifiche;
- Legge 31/12/1996 n. 676, recante delega al governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;
- DPR 28/07/1999, n. 318: Regolamento recante norma per l'individuazione delle misure di sicurezza minime per il trattamento dei dati personali;
- Legge 24/03/2001 n. 127, recante delega al governo per l'emanazione di un T.U. in materia di trattamento dei dati personali;
- Decreto legislativo 30/06/2003 n. 196 – Codice in materia di protezione dei dati personali, in particolare:
    - Dell'articolo 4 (Definizioni)
    - Degli articoli da 28 a 30 (Soggetti che effettuano il trattamento);
    - Degli articoli dal 31 al 36 (Misure di sicurezza) compresa abrogazione art. 34 (obbligo stesura DPS);
    - Degli articoli 59 e 60 (Disposizioni relative a specifici settori - Trattamento in ambito pubblico);
    - Degli articoli 95 e 96 (Disposizioni relative a specifici settori - Istruzione);
    - Dell'articolo 180 (Disposizioni transitorie - Misure di sicurezza);
    - Dell'allegato B (Disciplinare tecnico in materia di misure minime di sicurezza);
    - il DL n. 5/2012

Il DPS tiene presente la definizione di trattamento di dati forniti dall'art. 4 del D. Lgs 30 giugno 2003 n.196 che fa riferimento a qualunque operazione o complesso di operazioni 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".

Scopo di questo documento è di disegnare il quadro delle misure di sicurezza, organizzative, fisiche e logiche da adottare per il trattamento dei dati personali effettuato **dall'Istituto Comprensivo Statale di san Paolo d'Argon**

Conformemente a quanto prescrive il punto 19 del Disciplinare tecnico allegato sub b) al D.lgs. 196/2003, nel presente documento si forniscono idonee informazioni divise nelle seguenti tabelle:

Tabella 1 – Struttura organizzativa

Ha lo scopo di descrivere l'Istituzione scolastica evidenziando il nome e il tipo di scuola, la presenza di plessi o succursali, l'indirizzo e i dati utili per individuare il Dirigente Scolastico e i suoi principali collaboratori.

Tabella 2 – Informazioni di base – Tipologia dei dati trattati

Sono descritte in modo sintetico i compiti e le relative responsabilità in relazione ai trattamenti effettuati da questa Istituzione Scolastica direttamente o attraverso collaborazioni esterne, indicando anche la natura dei dati trattati (comuni, sensibili, giudiziari) e la struttura che operativamente effettua il trattamento. In questo quadro, la tabella 2 riporta le seguenti indicazioni:

ATTIVITA' – descrizione sintetica: ogni trattamento di dati viene legato all'attività a cui afferisce che dunque viene descritta sinteticamente: ad es. attività di "gestione dati alunni e genitori", "gestione dati personale", gestione dati DSGA" ecc.;

Natura dei dati trattati: per ogni trattamento viene indicato il tipo di dati trattati.

Viene indicato se sono presenti dati sensibili o giudiziari, oltre agli altri dati personali (cosiddetti dati Comuni);

INTERESSATI – persone a cui i dati si riferiscono: per ogni trattamento vengono indicate anche le diverse categorie di interessati, vale a dire le persone a cui i dati si riferiscono. Ad es. dati relativi a "alunni e genitori", "personale docente", "personale ATA" ecc.;

STRUTTURE DI RIFERIMENTO:questa voce indica la struttura (interna o esterna) che si occupa dei trattamenti di volta in volta indicati. Ad es. trattamenti di dati effettuati da "Area Segreteria" , "DSGA", "Dirigente Scolastico", "Docenti" "Addetto esterno alla manutenzione" ecc.

Tabella 3a – Banche dati, uffici di riferimento, operazioni effettuate

Attraverso questa tabella le attività identificate nella Tabella 2 vengono associate alle Banche dati elettroniche utilizzate per lo svolgimento di quelle stesse attività. Nella presente tabella vengono pertanto indicati:

Banche dati: Banche dati (ovvero data base o gli archivi informatici) attraverso cui sono gestiti i dati afferenti ad un determinato trattamento (ad es. l'attività di "gestione dati alunni e genitori" si effettua anche attraverso una banca dati elettronica),

Ubicazione fisica dei supporti di memorizzazione: contiene l'indicazione del luogo in cui risiedono fisicamente i dati, vale a dire dove si trova (in quale sede o in quali uffici), l'elaboratore sui cui dischi sono memorizzati. I dati, oppure i luoghi di conservazione dei supporti magnetici utilizzati per le copie di sicurezza (CD,DVD, ecc) ed ogni altro supporto rimovibile.

Applicazione: per ogni singola Banca Dati individuata, viene indicato anche il relativo programma applicativo per computer utilizzato. Ad esempio una Banca Dati contenente le lettere inviate dall'ufficio del personale viene gestita attraverso l'applicativo MS Word, oppure è il caso delle Banche Dati relative agli alunni e ai genitori, gestite attraverso l'applicativo ARGO.

Strutture che si occupano del trattamento: per ogni banca dati individuata si indicano le strutture (quella principale e le altre eventuali concorrenti) che si occupano, del trattamento. Ad esempio della Banca dati contenente i dati del personale si occupa principalmente il personale della Segreteria Amm.va ma vi può accedere anche il DSGA.

Trattamenti effettuati: per ogni Banca dati e per ogni struttura che effettua un trattamento di dati vengono descritti i compiti e le operazioni effettuate. Le operazioni possibili sono state raggruppate in sei categorie: comunicazione, consultazione, cancellazione, raccolta-inserimento, organizzazione, diffusione dei dati personali.

Tabella 3b – Dati cartacei, uffici di riferimento

In questa sezione vengono riportate le stesse informazioni relative a documenti cartacei.

Tabella 4 – Dispositivi di accesso

Nella Tabella 3 sono state individuate le banche dati e gli archivi elettronici contenenti dati personali.

Attraverso la Tabella 4 vengono descritte le caratteristiche principali dei dispositivi di accesso a quei dati, vale a dire dei PC attraverso cui è possibile accedere alle Banche dati elettroniche. I dati che vengono presi in considerazione sono i seguenti:

La tipologia: vale a dire se si tratta di un PC stand alone, di un server, di un client, ecc;

Il numero di inventario: che serve per identificare univocamente la macchina;

Il sistema operativo: Ad esempio Windows XP – 2003 Server -

Tipo di rete: Ad esempio se si tratta di una rete locale, se è connessa a Internet ecc.

Antivirus: vengono descritte le caratteristiche dell'antivirus utilizzato.

Tabella 5 – Analisi dei rischi

Una volta individuati, nelle Tabelle che precedono, i trattamenti dei dati effettuati dall'Istituzione Scolastica, le operazioni svolte dalla strutture preposte al trattamento, le banche dati e i relativi strumenti di accesso, attraverso la presente tabella vengono individuati i principali eventi potenzialmente dannosi per la sicurezza dei dati, ne vengono valutate le possibili conseguenze e la gravità in relazione al contesto fisico ambientale di riferimento.

A questo fine, la Tabella 5 prende in considerazione:

L'elenco degli eventi: contiene un elenco di eventi che possono generare danni e che comportano quindi rischi per la sicurezza dei dati personali.

La lista di eventi presa in considerazione è quella suggerita dal Garante della Privacy e si rifà a tre macrocategorie riconducibili a: eventi legati ai comportamenti degli operatori (ad esempio sottrazione delle credenziali di autenticazione, disattenzione, errori materiali ecc.), eventi concernenti gli strumenti (ad esempio azione di virus informatici, malfunzionamento degli strumenti, ecc.), eventi concernenti la situazione fisico ambientale (ad esempio ingressi non autorizzati a locali ad accesso ristretto, guasto dell'impianto elettrico ecc.);

Impatto sulla sicurezza dei dati: contiene una stima della conseguenza individuate per la sicurezza dei dati; a proposito di ciascun evento è fatta una valutazione della probabilità di accadimento e della gravità delle conseguenze.

TABELLA 6 – Le misure adottate

Una volta fatta l'analisi dei rischi va individuato le misure che l'Istituzione Scolastica ha adottato (o ha in programma di adottare) per contrastare i rischi connessi agli eventi dannosi individuati.

Misure: sono interventi tecnici o organizzativi attuati per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia; le misure individuate discendono in primo luogo dalle prescrizioni dell'Allegato B del Codice (ad esempio l'attribuzione di password di accesso personali, istruzioni per la custodia e l'uso dei supporti rimovibili, ecc.)

Prevenzione dei rischi: attraverso la tabella 6 le diverse misure atte a contrastare i rischi vengono correlate con gli eventi potenzialmente danno descritti nella tabella 5; ad esempio, l'adozione di un antivirus è una misura che viene

correlata alla prevenzione dei danni derivanti dagli eventi relativi agli strumenti (uno di questi è o può essere l'azione di virus informatici).

Attività Interessate – strutture e funzioni addette: le misure adottate hanno riflessi sulla sicurezza delle attività svolte evidenziate nella Tabella 2: per questo motivo le misure vengono correlate con le diverse attività interessate e con la struttura o la funzione responsabile o preposta alla sua adozione, ad esempio l'accesso controllato agli archivi contenenti dati sensibili è una misura organizzativa adottata dal DSGA.

Tabella 7 – Criteri e modalità di ripristino della disponibilità dei dati

Nella presente Tabella 7 sono descritti i criteri e le procedure adottate per il ripristino dei dati in caso di loro danneggiamento o di inaffidabilità della base dati.

Le informazioni che sono descritte sono le seguenti:

Banca dati: vengono innanzitutto indicate le banche dati. I data base o gli archivi interessati dalla procedura di back-up e ripristino dei dati;

Modalità di custodia delle copie: vengono indicate le modalità attraverso cui sono custodite le copie dei dati salvati (ad esempio cassaforte o armadio blindato);

Struttura o persone incaricate del salvataggio: viene indicata la struttura o le persone incaricate di effettuare il salvataggio e/o di controllarne l'esito.

Procedure per il salvataggio e il ripristino dei dati: in questa sezione vengono descritte sinteticamente le procedure e i criteri individuati per il salvataggio e il ripristino dei dati;

Pianificazione delle prove di ripristino: si indicano i tempi previsti per effettuare i test di efficacia delle procedure di salvataggio/ripristino dei dati adottate;

Periodicità del back-up: per indicare gli intervalli di tempo che passano tra un salvataggio ed un altro.

Tabella 8 – Pianificazione degli interventi formativi

Attraverso la Tabella 8 sono descritte le informazioni necessarie per individuare il quadro sintetico degli interventi formativi che si prevede di svolgere.

Le informazione che sono descritte sono le seguenti:

Descrizione sintetica degli interventi formativi: vengono descritti sinteticamente gli obiettivi e le modalità dell'intervento formativo;

Classi di incarico o tipologie di incaricati interessati: si indicano le classi omogenee di incarico a cui l'intervento è destinato e/o le tipologie di incaricati interessati, anche in riferimento alle strutture di appartenenza.

Tempi previsti per lo svolgimento degli interventi formativi.

Tabella 9 – Trattamenti affidati all'esterno

Questa tabella serve per redigere un quadro sintetico delle attività affidate a terzi che possono comportare il trattamento di dati, con l'indicazione di massima del quadro giuridico o contrattuale (nonché organizzativo e tecnico) in cui tale affidamento si inserisce, in riferimento agli impegni assunti per garantire la protezione dei dati stessi.

Le informazioni riguardano:

Indicazioni delle attività coinvolte: che serve per indicare sinteticamente quali attività potrebbero essere coinvolte in caso di affidamento di servizi all'esterno (è chiaro che, ad esempio, una manutenzione generale di tutti i PC potrebbe coinvolgere tutte le attività svolte con l'ausilio di strumenti informatici).

Trattamenti di dati interessati: indica i trattamenti di dati sensibili o giudiziari, effettuati nell'ambito della predetta attività (è possibile, per stare all'esempio fatto, che il tecnico manutentore abbia la necessità di accedere alle Banche dati per fare un test e dunque debba poter consultare i dati).

Soggetto esterno**:** è la società, l'ente o il consulente cui è stata affidata l'attività;

Descrizione degli impegni: impegni assunti o indicazioni date al soggetto esterno che effettua il trattamento.

Tabella 1 - Struttura organizzativa

FUNZIONE	DATI
Titolare del trattamento dati **ISTITUTO COMPRENSIVO STATALE** **Legale Rappresentante** Dirigente Scolastico: Prof. Vincenzo Demichele	***ISTITUTO COMPRENSIVO STATALE*** ***Via LOCATELLI 3- SAN PAOLO D'ARGON – BG -*** ***tel. 035/958054– tel/fax 035/958016*** ***e-mail: bgic870003@pec.istruzione.it*** N° sez. staccate 1 Polo scolastico di Cenate Sotto
Responsabile del Trattamento Dati: **Direttore dei Servizi Generali e Amm.vi** *Giovanna Francioni*	
Incaricati del Trattamento: *Personale ATA e Docenti*	

Tabella 2 - Informazioni di base

DISTRIBUZIONE DEI COMPITI E DELLE RESPONSABILITA'

STRUTTURA	RESPONSABILE del TRATTAMENTO	Trattamenti effettuati dalla struttura
Ufficio D.S.G.A.	D.S.G.A.	Trattamenti strumentali allo svolgimento dei compiti istituzionali, in materia di gestione contabile e amministrazione.
Ufficio DIRIGENTE SCOLASTICO	DIRIGENTE SCOLASTICO	Trattamenti strumentali allo svolgimento dei compiti istituzionali, predisposizione ed erogazione dell'Offerta Formativa
Segreteria DIDATTICA	D.S.G.A.	Trattamenti strumentali allo svolgimento dei compiti istituzionali in materia di: Iscrizioni alunni, assenze, acquisizione e rilascio certificati, gestione dati riguardanti stato di salute o altri dati di natura sensibile, gestione rapporti con alunni e famiglie, svolgimento pratiche infortuni, registrazione e consultazione carriera scolastica, tenuta archivio didattico. Gestione della corrispondenza ricevuta e inviata; tenuta del protocollo generale con conseguente registrazione della posta; della posta elettronica e dei documenti ricevuti via fax; elezioni e convocazioni Organi Collegiali.
Segreteria AMMINISTRATIVA	D.S.G.A.	Trattamenti strumentali allo svolgimento dei compiti istituzionali, in materia di selezione ed amministrazione del personale: registrazione delle assenze per malattia, motivi personali o familiari, espletamento funzioni politiche o sindacali, tenuta fascicoli personali. Trattamento dati relativi ad aspetti economici e previdenziali di tutto il personale scolastico. Gestione rapporti con fornitori, altri Enti pubblici e privati, redazione contratti esterni, emissione ordini.

Tabella 2 - Tipologia dei dati trattati

ATTIVITA'	Natura dei Dati Trattati			INTERESSATI	STRUTTURE DI RIFERIMENTO	RUOLO
	Dati Comuni	Dati Sensibili	Dati Giudiziari			
Gestione dati del DSGA	Si	Si	Si	Dsga	- Area Segreteria - Addetto esterno manutenzione -Dirigente Scolastico - Dsga	- Principale - Concorrente - Concorrente - Concorrente
Gestione dati del Dirigente Scolastico	Si	Si	Si	Dirigente Scolastico	- Area Segreteria - Addetto esterno manutenzione -Dirigente Scolastico - Dsga	- Principale - Concorrente - Concorrente - Concorrente
Gestione dati degli Alunni e dei Genitori	Si	Si	Si	Alunni e Genitori	- Area Segreteria - Addetto esterno manutenzione -Dirigente Scolastico - Dsga	- Principale - Concorrente - Concorrente - Concorrente
Archivio e Protocollo	Si	Si	Si	Alunni e genitori Personale Docente Personale ATA Fornitori	- Area Segreteria -Dirigente Scolastico - Dsga	- Principale. - Concorrente - Concorrente
Gestione dati del Personale (ATA E DOCENTE)	Si	Si	Si	Personale docente Personale ATA	- Area Segreteria - Addetto esterno manutenzione -Dirigente Scolastico - Dsga	- Principale - Concorrente - Concorrente - Concorrente
Gestione dati Contabili e Finanziari	Si	Si	Si	Personale Docente Personale ATA Fornitori	- Area Segreteria - Addetto esterno manutenzione -Dirigente Scolastico - Dsga	- Principale. - Concorrente - Concorrente - Concorrente

Tabella 3a - Banche dati, uffici di riferimento, operazioni effettuate

Banche dati relative all'attività **Gestione dati CONTABILITA' Finanziaria – UFFICIO DEL D.S.G.A.**										
Banche Dati	**Ubicazione Fisica dei supporti di Magnetizzazione**	**Applica-zioni**	**Struttura**	**Ruolo**	**Comuni-cazione**	**Consul-tazione**	**Cancella-zione**	**Raccolta e inseri-mento**	**Organiz-zazione**	**Diffu-sione**
-Contabilità/ Bilancio -Anagrafico Fornitori	Stanza - uff. DSGA **Responsabile DSGA:** **Sig.ra Giovanna Francioni**	Axios SIDI	UFF. DSGA	Principale	Si	Si	Si	Si	Si	Si

Banche dati relative all'attività **Svolgimento compiti istituzionali, predisposizione ed erogazione P.O.F.- UFFICIO DEL D.S.**										
Banche Dati	**Ubicazione Fisica dei supporti di Magnetizzazione**	**Applica-zioni**	**Struttura**	**Ruolo**	**Comuni-cazione**	**Consul-tazione**	**Cancella-zione**	**Raccolta e inseri-mento**	**Organiz-zazione**	**Diffu-sione**
Cartella Documenti	Stanza Uff. DIRIGENTE SCOLASTICO **D.S. Prof. Vincenzo Demichele**	SIDI	UFF. D.S.	Principale	Si	Si	Si	Si	Si	Si

Tabella 3a - Banche dati, uffici di riferimento, operazioni effettuate

Banche dati relative all'attività **Gestione dati Alunni e Genitori Plesso Elementari e Plesso Medie – SEGRETERIA DIDATTICA**

Banche Dati	Ubicazione Fisica dei supporti di Magnetizzazione	Applica-zioni	Struttura	Ruolo	Comuni-cazione	Consulta-zione	Cancel-lazione	Raccolta e inseri-mento	Organiz-zazione	Diffu-sione
Cartella Documenti (Alunni/Genitori) C.T.P.	Stanza Segreteria **Incaricato** • **Stefania Arrigoni** • **Silvana Trevisan**	Axios-Sidi	-Segreteria Didattica	Principale	Si	Si	Si	Si	Si	Si
			-Dsga	Concorrente	Si	Si	Si	Si	Si	Si
Anagrafico Alunni/Genitori Scuola EE - MM	Stanza Segreteria **Incaricato** • **Stefania Arrigoni** • **Silvana Trevisan**	Axios-Sidi	-Segreteria Didattica	Principale	Si	Si	Si	Si	Si	Si
			-Dsga	Concorrente	Si	Si	Si	Si	Si	Si

Banche dati relative all'attività **Gestione Protocollo/Posta Elettronica**

Banche Dati	Ubicazione Fisica dei supporti di Magnetizzazione	Applica-zioni	Struttura	Ruolo	Comuni-cazione	Consulta-zione	Cancella-zione	Raccolta e inseri-mento	Organiz-zazione	Diffu sione
Gestione Protocollo	Stanza Segreteria **Incaricato** • **Stefania Arrigoni** • **Silvana Trevisan**	Axios-Sidi	-Segreteria Didattica	Principale	Si	Si	Si	Si	Si	Si
			-Dsga	Concorrente	Si	Si	Si	Si	Si	Si
Posta Elettronica	Stanza Segreteria **Incaricato** • **Stefania Arrigoni** • **Silvana Trevisan**	Outlook	-Segreteria Didattica	Principale	Si	Si	Si	Si	Si	Si
			-Dsga	Concorrente	Si	Si	Si	Si	Si	Si
Cartella Documenti (Corrispondenza, miscellanee varie)	Stanza Segreteria **Incaricato** • **Stefania Arrigoni** • **Silvana Trevisan**	Server	-Segreteria Didattica	Principale	Si	Si	Si	Si	Si	Si
			-Dsga	Concorrente	Si	Si	Si	Si	Si	Si

Tabella 3a - Banche dati, uffici di riferimento, operazioni effettuate

Banche dati relative all'attività **Gestione Fiscale e Retribuzioni – SEGRETERIA AMMINISTRATIVA /CONTABILITA'**										
Banche Dati	**Ubicazione Fisica dei supporti di Magnetizzazione**	**Applica-zioni**	**Struttura**	**Ruolo**	**Comuni-cazione**	**Consulta-zione**	**Cancel-lazione**	**Raccolta e inseri-mento**	**Organiz-zazione**	**Diffu-sione**
-Retribuzioni -Gest Fiscale - Bilancio	Stanza Ufficio Dsga Direttore Amm.vo	Axios-Sidi	-Segreteria Amm.va -Dsga	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si
Cartella Documenti (Retribuzioni, Gestione Fiscale)	Stanza Ufficio Dsga Segreteria Amministrativa **Incaricato: Alfonsa Vaianella**	Axios-Sidi	Segreteria Amm.va Dsga	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si

Banche dati relative all'attività **Gestione C/C – SEGRETERIA AMMINISTRATIVA**										
Banche Dati	**Ubicazione Fisica dei supporti di Magnetizzazione**	**Applica-zioni**	**Struttura**	**Ruolo**	**Comuni-cazione**	**Consul-tazione**	**Cancella-zione**	**Raccolta e inseri-mento**	**Organiz-zazione**	**Diffu-sione**
Area -Gest Fiscale	**Incaricato: Alfonsa Vaianella**	Axios	Segreteria Amm.va Dsga	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si

Banche dati relative all'attività **Gestione Fornitori / Area Magazzino - SEGRETERIA AMMINISTRATIVA**										
Banche Dati	**Ubicazione Fisica dei supporti di Magnetizzazione**	**Applica-zioni**	**Struttura**	**Ruolo**	**Comuni-cazione**	**Consul-tazione**	**Cancella-zione**	**Raccolta e inseri-mento**	**Organiz-zazione**	**Diffu-sione**
-Area Magazzino -Anagrafico Fornitori	Segreteria Amministrativa **Incaricato: Caccia Laura**	Axios	Segreteria Amm.va Dsga	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si
Cartella Documenti Magazzino, Fornitori e Varie	Segreteria Amministrativa **Incaricato: Caccia Laura**	Pacchetto Office	Segreteria Amm.va Dsga	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	S Si	Si Si

Tabella 3a - Banche dati, uffici di riferimento, operazioni effettuate

Banche dati relative all'attività **Gestione dati Personale Docente a Tempo Determinato Scuola Media ed Elementare - SEGRETERIA DEL PERSONALE**

Banche Dati	Ubicazione Fisica dei supporti di Magnetizzazione	Applica-zioni	Struttura	Ruolo	Comuni-cazione	Consul-tazione	Cancella-zione	Raccolta e inseri-mento	Organiz-zazione	Diffu-sione
Anagrafico Personale T.I. Scuola EE Scuola MM	Stanza Segreteria Personale 1^ e 2^ piano **Incaricato** • **Alfosa Vaianella** • **Maria Luisa Zambelli** • **Criastina Consoli**	Axios Sidi	Area Segreteria Dsga.	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si
Cartella Documenti (Personale Docente)	Stanza Segreteria Personale 1^ e 2^ piano **Incaricato** • **Alfosa Vaianella** • **Maria Luisa Zambelli** • **Criastina Consoli**	Axios Sidi	Area Segreteria Dsga	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si

Banche dati relative all'attività **Gestione dati Personale Docente di Ruolo Scuola Media ed Elementare – SEGRETERIA DEL PERSONALE**

Banche Dati	Ubicazione Fisica dei supporti di Magnetizzazione	Appli-cazioni	Struttura	Ruolo	Comuni-cazione	Consul-tazione	Cancella-zione	Raccolta e inseri-mento	Organiz-zazione	Diffu-sione
Anagrafico Personale T.D. Scuola EE Scuola MM	Stanza Segreteria Personale **Incaricato** • **Alfosa Vaianella** • **Maria Luisa Zambelli**	Axios Sidi	Area Segreteria Dsga	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si

	• **Criastina Consoli**									
Cartella Documenti (Personale Docente)	Stanza Segreteria Personale **Incaricato** • **Alfosa Vaianella** • **Maria Luisa Zambelli** • **Criastina Consoli**	Axios Sidi	Area Segreteria Dsga	Principale Concorrente	Si Si	Si Si	Si Si	Si Si	Si Si	Si Si

Banche dati relative all'attività **Gestione dati Laboratori informatica –**

Ubicazione Fisica dei supporti di Magnetizzazione	SISTEMA OPERATIVO	Presenza di Password	Antivirus Free	Screen saver	Gruppo di continuità	Connessione internet	SERVER	APPLICAZIONI	
Stanza Laboratorio Informatica Sc. Primaria San Paolo **Incaricato: Bacher Elena**	WINDOWS XP	SI	si	Si	NO	ADSL	WINDOWS Server 2003	Open Office	
Scuola Primaria Tutte le classi **Incaricati: Docenti della classe**	VISTA WINDOWS 7	SI	si	Si	no	Si	no	Open Office	
Sc. Secondaria San Paolo Sala Professori n. 2 **Incaricato: Pesenti Mario** Aule n. 9 **Incaricati: Docenti della classe**	 WINDOWS7 Windows xp-vista WINDOWS 7	SI	si	Si	NO	ADSL	WINDOWS Server 2003	Open Office	
Stanza Laboratorio Informatica Polo Scolastico Cenate • Primaria: Bettoni Cesare • Secondaria: Caldara Paola Tutte le classi **Incaricato: Docenti della classe**	Windows XP Windows XP	SI SI	si	Si	NO	ADSL	WINDOWS Server 2003	Open Office	
Scuola infanzia **Incaricato: Docenti sezione**	WINDOWS xp XP	SI	si	Si	NO	ADSL	no	Open Office	

Tabella 3b - Dati cartacei, uffici di riferimento

UBICAZIONE DATI CARTACEI				PERCENTUALE DI RISCHIO		
Collocazione	**Numerazione/ Inventario**	**Incaricati del Trattamento Dati Sensibili**	**Dati Sensibili e/o personali, giudiziari**	**Alta**	**Media**	**Bassa**
Presidenza	Armadio 1 e 2	Demichele Vincenzo Francioni Giovanna	- Documenti d'Istituto - Doc. per la sicurezza e la salute durante il lavoro - Verbali collegio docenti - Modulistica gite		X X	

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA - 2015

Tabella 3b - Dati cartacei, uffici di riferimento

UBICAZIONE DATI CARTACEI				PERCENTUALE DI RISCHIO		
Collocazione	**N. INV.**	**Incaricati del Trattamento Dati Sensibili**	**Dati Sensibili e/o personali, giudiziari**	**Alta**	**Media**	**Bassa**
Uff.DSGA	N°1 armadio con chiavi	ASS.TI AMM.VI :Vaianella A.-Caccia Laura	- Documenti uniemens - DMA - Documenti Contabili - Mandati e Reversali - Registri verbali consiglio di isituto e giunta esecutiva		X	
	n.2 armadio con chiavi		- Documenti inventario beni mobili - Documenti TFR		X	
<u>Segreteria Area personale</u>	STANZA PIANO SUPERIORE ARCHIVIO CORRENTE N°13 (ARMADIO BASSO)	ASS.TI AMM.VI : Maria Luisa Zambelli Cristina Consoli	Armadio - Permessi L104 - Rilevazioni assenze anagrafe prestazioni - Permessi ATA		X	
	N°14 (ARMADIO)		- Graduatorie interne - Controllo veridicità - Messe a disposizione		X	
	N°8 (schedario con chiavi)		TITOLARIO Assenze del personale		X	
	SEGRATERIA PIANO INFERIORE N° 4 (Armadio con chiavi)	ASS.TI AMM.VI : Silvana Trevisan Stefania Arrigoni Alfonsa Vaianella Maria Luisa Zambelli Cristina Consoli Caccia Laura	- Domanda inclusione graduatorie			

	N°5 (Armadio con chiavi) N°6 (Armadio con chiavi) N°7 (Armadio con chiavi) N°9 (schedario con chiavi) N°10 (Armadio con chiavi) N°11 (Armadio con chiavi) N°12 (Armadio con chiavi)		- Trasferimenti - Utilizzazioni - Permessi di diritto allo studio - Compensi accessori - Fascicoli personale in uscita - Fascicoli personale ATA - Registri permanenti del personale - Titolario protocollo - Fascicoli personale di ruolo			
<u>Segreteria Area didattica/protocollo</u>	N° 1 (Armadio con chiavi)		- Fascicoli personali alunni H - Faldoni infortuni - Viaggi d'istruzione - Organi collegiali - Registri perpetui diplomi - Diplomi anni precedenti - Materiale stage - Registri perpetui diplomi			

	N° 2 (Armadio con chiavi) N° 3 (Armadio senza chiave) N° 13 (Cassaforte)	ASS.TI AMM.VI : Silvana Trevisan Stefania Arrigoni Alfonsa Vaianella Maria Luisa Zambelli Cristina Consoli Caccia Laura	- Informazioni di contesto INVALSI - Modulistica varia - Rilevazioni alunni annuali - Elenchi vari alunni plessi - Scrutini ed esami perpetui - Materiale didattico - Fascicoli alunni per plesso - Diplomi anno corrente - Timbro ministeriale			
ARCHIVIO STORICO	Scaffale N°		- Cud personale a T.D. - Cud personale di RUOLO - Graduatorie Scuola media/elem. - Fascicoli alunni - Stato personale Docenti a T.D. - Fascicoli Docenti a T.D. - Registri Protocollo - Registri Certificati Alunni - Documentazione alunni Fascicoli DOCENTI e ATA documentazioni varie Documenti , fascicoli ,registri , elaborati Dal 1970			

Tabella 4 - Dispositivi di accesso

Tipologia	Postazione	Sistema Operativo	Internet	RAM	Anno	Dispositivo	Archivio

			Exstranet		Costruzione	Antivirus	
Server	Stanza archivio	Windows Server 2008 R2	Si	4 gb	2013	KARSPESKY endpoint security 10	DATABASE axios / share folder / share printer
Client	Presidenza	Windows 7 Pro	Si	4 gb	2013	KARSPESKY endpoint security 10	Infozeta-registro elettronico / share folder server
Client	Direzione amm.va	Windows 8 Pro XP Professional	Si	4 gb	2014	KARSPESKY endpoint security 10	Axios / share folder server
2 Client	Segreteria didattica	2 Pc - Win 8 Pro	Si	4 gb	2014	KARSPESKY endpoint security 10	Axios / share folder server
3 Client	Segreteria amm.va	3 Pc - Win 8 Pro 1 Pc – Win Xp Pro	Si	4 gb	2014	KARSPESKY endpoint security 10	Axios / share folder server

Descrizione Qualitativa della Rete:

Struttura peer to peer. Nome Workgroup - No proxy, protetto da **Firewall**, accesso ad Internet mediante Router Ministeriale Connessione Fastweb.
La Scuola è dotata di una propria Rete Locale che permette di connettere e condividere tutti gli elaboratori presenti nell'ufficio al Server (ubicato nella stanza archivio) protetto da un gruppo di continuità da 650 VA. Il Server gestisce, controlla e autorizza tutti gli accessi e, il personale incaricato ha la possibilità di salvare sul server stesso, files contenenti dati sensibili, in una cartella condivisa.

Tab. 5 - Valutazione dei rischi

Tipologia	Eventi	Probabilità	Gravità
Strumenti	Accessi Esterni non Autorizzati	Bassa	Media
Contesto fisico ambientale	Accessi non Autorizzati Locali reparti ad accesso ristretto	Bassa	Media
Contesto fisico ambientale	Asportazione furto di strumenti contenenti dati	Bassa	Bassa
Strumenti	Azione Virus informatico di codici malefici	Media	Media

Comportamento degli operatori	Carenza di consapevolezza, disattenzione incuria	bassa	Bassa
Comportamento degli operatori	Comportamenti sleali o fraudolenti	bassa	Bassa
Comportamento degli operatori	Errore materiale	Media	Media
Contesto fisico ambientale	Errori umani nella gestione della sicurezza fisica	bassa	Media
Contesto fisico ambientale	Eventi distruttivi naturali artificiali, dolosi,accidentali dovuti ad incuria	Bassa	Media
Comportamento degli operatori	Furto di credenziali di autenticazione	bassa	Bassa
Contesto fisico ambientale	Guasto ai sistemi complementari (impianto elettrico)	bassa	Media
Strumenti	Malfunzionamento, o degrado degli strumenti	bassa	Media
Comportamento degli operatori	Smarrimento di credenziali e autenticazione	bassa	Bassa
Strumenti	Spamming o altre tecniche di sabotaggio	bassa	Media

Tabella 6 – MISURE ADOTTATE

Tipologia Trattamenti: con strumenti informatici

L'accesso al database è protetto con credenziali di autenticazione
Ad ogni incaricato sono assegnate credenziali personali di autenticazione (Username e Password)
La password è almeno di 8 caratteri
Sono impartite istruzioni agli incaricati per la custodia e segretezza della password
La password è conosciuta solo dall'incaricato
Sono impartite istruzioni agli incaricati per la modifica della parola chiave almeno ogni tre mesi
La protezione avviene attraverso un antivirus di rete

I principali programmi utilizzati (windows) sono sempre aggiornati almeno annualmente per prevenire diretti e vulnerabilità.
Aggiornamento almeno semestrale in caso di trattamento di dati sensibili e giudiziali
E' stato stipulato un contratto di manutenzione con la Ditta Files Multimedia, ditta specializzata per la manutenzione delle componenti Hardware e software
E' stata adottata una procedura di backup giornaliera su Disco Rigido Esterno e Mensile su Disco Rigido del Server
Sono impartite istruzioni per la custodia e l'uso di supporti rimovibili su cui sono memorizzati i dati per prevenire per prevenire accessi non autorizzati

Tabella 6 – MISURE ADOTTATE

Tipologia Trattamenti: con strumenti informatici

Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati sensibili entro sette giorni in caso di danneggiamento dei dati o degli strumenti
I supporti removibili contenenti dati sensibili se non utilizzati sono distrutti o riutilizzati in maniera che le informazioni non siano più intellegibili
Alcuni documenti con dati sensibili o giudiziali sono affidati agli incaricati e ad essi sono impartite istruzioni scritte
Nelle suddette istruzioni si dispone che i documenti siano controllati e custoditi in maniera che ad essi non accedano persone prive di autorizzazioni.

Sono impartite istruzioni sulla sicurezza nelle lettere di incarico e nella designazione del responsabile del trattamento dati
Le lettere di incarico o di designazione degli incaricati vengono raccolte in modo ordinato e con cadenza annuale si procede ad aggiornare i dati
Nelle istruzioni agli incaricati si dispone che i documenti siano restituiti al termine delle operazioni affidate
Esiste un piano di formazione degli incaricati
Vi sono verifiche periodiche su trattamenti di dati non consentiti e non corretti o non necessari
L'ingresso dei locali dove avvengono i trattamenti e dove sono custoditi i dati è sempre controllato

Tabella 6 – MISURE ADOTTATE

Ai dati non possono accedere persone non autorizzate
Al termine dell'orario di ufficio, o quando non è più possibile la vigilanza degli incaricati, i locali dove risiedono i dati vengono chiusi a chiave
Esiste un sistema di allarme antintrusione a protezione dei locali dove sono custoditi i dati
I documenti sono custoditi in classificatori o armadi chiusi a chiave
Sono presenti dispositivi antincendio (estintori a norma)
Sono presenti distruggidocumenti per garantire la massima riservatezza all'interno degli uffici.
Sono impartite istruzioni ed effettuati controlli sull'operato di soggetti esterni che possono venire a contatto con dati trattati dall'istituto
Sono state applicate sbarre alle finestre a protezione dei locali dove sono contenuti i dati ????????

Tabella 7 – criteri e modalità di ripristino delle disponibilità dei dati

Banca Dati	Periodicità	Modalità di custodia delle copie	Incaricato	Procedura di salvataggio e ripristino	Pianificazione Prove di ripristino
Anagrafico Alunni e Famiglie Cartella Documenti Sensibili	Giornaliero	PC SERVER	Ass.te amm.vo	Hard Disk- esterno USB	giornaliero
Anagrafico personale Docente e Ata Cartella Documenti Sensibili	Giornaliero	PC SERVER	Ass.te amm.vo	Hard Disk- esterno USB	giornaliero

Tabella 7 – criteri e modalità di ripristino delle disponibilità dei dati

Contabilità e Bilancio Cartella Documenti Sensibili	Giornaliero	PC SERVER C:\	Addetto esterno manutenzione informatica	Hard Disk esterno USB	giornaliero
Retribuzioni Cartella Documenti Sensibili	Giornaliero	PC SERVER C	Addetto esterno manutenzione informatica	Hard Disk esterno USB	giornaliero
Magazzino - Fornitori Cartella Documenti Sensibili	Giornaliero	PC SERVER C	Addetto esterno manutenzione informatica	Hard Disk esterno USB	giornaliero
Gestione Fiscale Cartella Documenti Sensibili	Giornaliero	PC SERVER C	Addetto esterno manutenzione informatica	Hard Disk esterno USB	giornaliero

Tabella 8 – Formazione svolta e pianificazione degli interventi formativi

Intervento	Incaricati interessati	Modalità di fruizione e durata
D.lgs 196/2003 principi generali regole d'applicare ai trattamenti operati dalla PA Disciplinare tecnico (Misure minime di sicurezza)	Tutti i Titolari di credenziali di autenticazione	Anno solare

Tabella 9 – Trattamenti Affidati All'esterno

Attività	Soggetto esterno	Impegni
Manutenzione hardware e software, gestione sicurezza e ripristino dati	Ditta	La Ditta si impegna a rispettare le istruzioni specifiche ricevute per il trattamento dei dati, a relazionare sulle misure di sicurezza adottate e ad informare il Titolare del trattamento in caso di situazioni anomale o emergenze.
Sito Web e Sistema informatizzato del Registro Elettronico di classe e del professore	Infozeta	L'Istituto è dotato di un registro elettronico INFOZETA nel quale sono contenuti i dati relativi al registro di classe e al registro personale del professore. In attesa di poter esprimere il previsto parere sui provvedimenti attuativi del Ministero dell'Istruzione riguardo all'iscrizione on line degli studenti, all'adozione dei registri on line e alla consultazione della pagella via WEB, il garante auspica l'adozione di adeguate misure di sicurezza a protezione dei dati. La sicurezza e la privacy, nonché le diverse tipologie di dati consultabili in funzione delle prerogative di accesso (Dirigente,Docente,Famiglia,ecc), sono controllati da INFOZETA mediante chiavi di accesso individuali, generate da una apposita procedura interna e comunicabili ai destinatari a mezzo di posta elettronica o cartacea. Le richieste provenienti dalle utenze sono indirizzate ai nostri server, che fanno da intermediari dei flussi dati informatici e garantiscono protezione e affidabilità funzionali. Il sito dell'Istituto Comprensivo in cui si appoggia il Registro Elettronico si avvale del protocollo internazionale https (Hyper Text Transfer Protocol over Secure Socket Layer) di crittografia asimmetrica e viene utilizzato per garantire trasferimenti riservati di dati nel WEB, in modo da impedire intercettazioni dei contenuti tramite la tecnica di attacco del "man in the middle".

Nel pieno rispetto delle vigenti disposizioni in materia di trattamento, la DSGA, ***incaricato del trattamento dei dati***, in possesso delle necessarie competenze tecnico-professionali è stato nominato ***"Amministratore di Sistema"*** è preposto a compiti di vigilanza e controllo del corretto utilizzo del sistema informatico gestito e utilizzato dall'Istituto.
Il presente D.P.S. è sottoposto ad aggiornamento annuale , come previsto dalla regola 19 del Disciplinare Tecnico- L.vo n. 196/2003 e successive modifiche.
L'originale viene custodito presso la Dirigenza dell'Istituto e una copia consegnata al DSGA Responsabile del Trattamento dei dati.
Nella relazione accompagnatoria del bilancio di esercizio si riferisce dell'avvenuta redazione del presente documento per il 2013.

Protocollo n° 198/A.20/S del 14/01/2015
Firma del Rappresentante Legale **IL DIRIGENTE SCOLASTICO**

Firma del Responsabile del Trattamento dei Dati **IL D.S.G.A.**

DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA
(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici: Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.
2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.
4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.
5. La parola chiave, quando è prevista dal sistema di autenticazione, 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.
6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.
7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate , salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.
8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.
9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.
10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.
11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.
12. Sito Web Istituto e Registro elettronico- REGOLAMENTO D'USO E PRIVACY
13. Criteri, procedure per garantire l'integrita' dei dati
14. Custodia e conservazione delle copie di back-up
15. Protezione dai rischi durante la trasmissione dati
16. Criteri da adottare per garantire l'adozione delle misure minime di sicurezza nel caso di affidamento del trattamento a so
17. Affidamento a persone fisiche e a persone giuridiche

Sistema di autorizzazione

1. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.
2. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.
3. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

1. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
2. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.
3. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggere difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.
4. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.
5. Il sito dell'Istituto Comprensivo in cui si appoggia il Registro Elettronico si avvale del protocollo internazionale https (Hyper Text Transfer Protocol over Secure Socket Layer) di crittografia asimmetrica e viene utilizzato per garantire trasferimenti riservati di dati nel WEB, in modo da impedire intercettazioni dei contenuti tramite la tecnica di attacco del "man in the middle".

Documento programmatico sulla sicurezza

1. Ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari aggiorna il documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

l'elenco dei trattamenti di dati personali;

- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità di dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- 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;
- la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
- per i dati personali idonei a rilevare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

- I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici
- Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.
- I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.
- Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

Misure di tutela e garanzia

Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervallo effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l'ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell'incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

- Agli incaricati sono impartite istruzioni scritte 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. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.
- Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.
- L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Allegato 1 : Atto di adozione e approvazione del DPS

ISTITUTO COMPRENSIVO STATALE DI SAN PAOLO D'ìARGON

Delibera Consiglio di Istituto n. ……. del ……..

Adozione del Documento Programmatico sulla Sicurezza (DPS)

Il DIRIGENTE SCOLASTICO DELL'ISTITUTO COMPRENSIVO DI SAN PAOLO D'ARGON
PROF. VINCENZO DEMICHELE

- Visto il D.Lgs. 30 giugno 2003, n. 196 e successive modifiche ("Codice in materia di protezione dei dati personali") che disciplina la gestione di dati personali e sensibili da parte di privati e delle Pubbliche Amministrazioni;
- Considerato che detto Codice in materia di protezione dei dati personali introduce numerose e significative novità di ordine legale, normativo, procedurale e tecnologico, in materia di privacy e sicurezza, anche a carico delle Pubbliche Amministrazioni;
- Tenuto conto dell'importanza di assicurare un adeguato livello di privacy e sicurezza nelle banche dati e nei processi di trattamento dei dati personali e sensibili dei cittadini, delle aziende e delle altre Pubbliche Amministrazioni;
- Considerato che detto Codice prevede all'art. 30 la "tenuta di un Aggiornato documento Programmatico sulla Sicurezza";
- Ritenuto opportuno dotare l'Istituto di un documento unitario che possa fornire supporto metodologico, procedurale e operativo nella individuazione e messa in atto - nel rispetto di criteri di efficienza ed economicità - delle misure di sicurezza nei trattamenti dei dati operati dalle varie articolazioni organizzative dell'Istituto

DELIBERA

- di approvare ed adottare con decorrenza immediata il Documento Programmatico sulla Sicurezza dell'Istituto relativamente ai trattamenti di dati personali e sensibili svolti dall'Istituto;
- di dare atto che tutto il personale e i collaboratori dell'Istituto sono nominati incaricati del trattamento dei dati e sono tenuti a rispettare scrupolosamente quanto prescritto dal REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI .

San Paolo d'Argon,

Il Dirigente Scolastico
Prof. Vincenzo Demichele

Allegato 2: Atto del Dirigente Scolastico di nomina dei Responsabili del trattamento dei dati

Prot.n. ……./A20s del ……..

ATTO DI NOMINA DEI RESPONSABILI DEL TRATTAMENTO DEI DATI PERSONALI

- Il DIRIGENTE SCOLASTICO DELL'ISTITUTO COMPRENSIVO DI SAN PAOLO D'ARGON
- PROF. VINCENZO DEMICHELE
-
- Visto l'art. 29 del D.Lgs. 196/2003 e successive modifiche ed integrazioni,

NOMINA

il DSGA Francioni Giovanna

Responsabile del trattamento dei dati, per l'ambito di proprio competenza,

I compiti affidati ai Responsabili del trattamento dei dati, ai quali ciascun Responsabile si dovrà attenere scrupolosamente, sono analiticamente specificati per iscritto nella sezione "Istruzioni per i Responsabili del trattamento dei dati" del Documento Programmatico sulla Sicurezza, custodito a cura della Segreteria Generale, di cui si riporta un estratto:

(inizio estratto:)

II Responsabile del trattamento dei dati deve seguire scrupolosamente le disposizioni di seguito elencate:

1. assumere il compito di evadere le eventuali domande di accesso, di rettifica, di integrazione, di cancellazione e di blocco di dati, su istanza degli interessati del trattamento dei dati personali, ex art. 7 del D.Lgs. 196/2003;

2. vigilare, secondo le prassi istituite ed in accordo con gli altri collaboratori del Titolare, affinché gli incaricati al trattamento dei dati personali si attengano alle procedure di volta in volta indicate specificatamente, sia oralmente sia per iscritto, anche in relazione all'applicazione delle misure organizzative, fisiche e logiche sulla sicurezza del trattamento dei dati secondo il dettato del D.Lgs. 196/2003;

3. procedere - ove necessario - al rilascio ed alla revoca delle autorizzazioni previste dagli artt. 12,13 e 14 del Disciplinare Tecnico in materia di misure minime di sicurezza contenute nel D.Lgs. 196/2003, ed altresì a verificare e fare in modo che l'accesso ai dati da trattare, da parte degli incaricati, sia limitato a quelli strettamente necessari allo svolgimento delle mansioni loro assegnate;

4. impegnarsi a:

- individuare e censire le banche dati in formato elettronico e cartaceo
- designare per iscritto gli incaricati al trattamento dei dati, nell'ambito della propria Area di competenza, specificando analiticamente per iscritto i programmi applicativi, le cartelle ("directory") locali e di rete e gli archivi cartacei ai quali l'incaricato può avere accesso, specificando il tipo di accesso consentito (solo lettura/consultazione oppure gestione completa), ottemperando in questo modo all'art. 30 del D.Lgs. 196/2003, che richiede che "la designazione è effettuata per iscritto e individua puntualmente l'ambito del trattamento consentito");
- nominare, quali Responsabili del trattamento dei dati, i soggetti esterni (ditte, fornitori, software house, etc..) coinvolti nel processo di trattamento dei dati personali; nel caso si tratti di soggetti che collaborano con l'Istituto a titolo personale o come ditta individuale, sarà possibile inquadrare tali soggetti come incaricati del trattamento dei dati;
- comunicare tempestivamente all'Amministratore di Sistema ogni atto ed evento che comporti una disattivazione immediata o modifica dei profili e delle autorizzazioni di accesso alla banche dati e ai programmi applicativi, come ad esempio: dimissioni, assunzioni, trasferimenti da/verso altre Aree/Servizi, cessazione , sospensione o revoca di incarico, variazioni di ruolo/responsabilità, etc.;
- comunicare al Custode delle password di competenza, l'utilizzo di eventuali User ID e password necessarie per accedere a specifici software e/o servizi a cui il Area e/o il Settore di competenza si è regolarmente registrato;
- in merito al mantenimento delle autorizzazioni di cui al precedente punto 3, s'impegna a svolgere il compito di verificare - almeno una volta all'anno - la sussistenza delle condizioni che hanno determinato la loro emissione e, in caso di difetto, di procedere alla loro revoca ;
- collaborare, almeno una volta l'anno, alla redazione o all'aggiornamento della sezione del Documento Programmatico sulla Sicurezza di cui all'art. 19 dell'allegato B) del D.Lgs. 196/2003, relativa a tutti i criteri tecnici e organizzativi adottati nell'attività di trattamento dei dati da parte degli incaricati ed assistere, in base anche all'esperienza maturata, il Titolare e altre persone eventualmente indicate dal titolare nell'individuazione degli atri criteri di sicurezza, sia organizzativi sia fisici sia logici, nell'ambito del proprio Settore di competenza;
- vigilare sulla corretta gestione e sullo smaltimento dei supporti mobili di memorizzazione (come ad esempio floppy-disk, cd-rom, dvd, memorie flash rimovibili, etc.) secondo quanto previsto dal DPS e da apposite norme e regolamenti emessi dall'Istituto;
- far adottare, nell'ambito della propria Area di competenza, le ulteriori misure di sicurezza previste in caso di trattamento di dati sensibili o giudiziari, di cui agli artt. 20,21,22,23 e 24 del Disciplinare Tecnico;
- far adottare, nell'ambito dell'Area di competenza, le modalità previste in caso di trattamenti senza l'ausilio di strumenti informatici, di cui agli artt. 27,28° 29 del Disciplinare Tecnico; in particolare quando i documenti sono affidati agli incaricati, devono essere controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione e siano restituiti al termine delle operazioni affidate; nel caso di dati sensibili o giudiziari

l'accesso agli archivi deve essere controllato, e le persone che accedono dopo l'orario di chiusura devono essere identificate e registrate;

- assumere, nell'ambito dell'Area di competenza, il mandato a costituirsi, replicare, depositare documenti, opporsi e svolgere ogni altra attività difensiva necessaria in eventuali ricorsi presentati dall'interessato al trattamento , sia davanti al Garante - ex art. 8 e 9 del D. Lgs 196/2003 - sia davanti all'autorità giudiziaria ordinaria, e ciò anche in relazione alle controversie che potrebbero instaurarsi in materie di rilascio di eventuali autorizzazioni da parte del Garante;
- individuare le casistiche che richiedono l'invio di notifiche al Garante e, di concerto con gli altri Responsabili del trattamento dei dati e con il Titolare del trattamento dei dati, collaborare alla compilazione della necessaria modulistica . Si ricorda comunque che l'obbligo formale di effettuare la notificazione grava sul Titolare del trattamento, il quale deve richiedere che la notificazione sia sottoscritta anche dai Responsabili di competenza

(fine estratto)

In caso di aggiornamenti , integrazioni e modifiche del Documento Programmatico sulla Sicurezza sarà cura della Segreteria Generale comunicare una nuova versione del Documento Programmatico sulla Sicurezza - oppure la parte modificata - a ciascun Responsabile del trattamento dei dati.

In fase di prima adozione della normativa, i Responsabili del trattamento dei dati potranno chiedere supporto metodologico e procedurale alla Segreteria Generale.

Il presente provvedimento ha decorrenza dalla data di notifica dello stesso agli interessati.

Il Dirigente Scolastico
Prof. Vincenzo Demichele

Allegato 3: Atto del Dirigente Scolastico di nomina del Responsabile del trattamento dei dati con responsabilità di coordinamento e supervisione

Prot.n. ……/A20s del ……..

ATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI PERSONALI CON RESPONSABILITÀ' DI COORDINAMENTO E SUPERVISIONE

Il DIRIGENTE SCOLASTICO DELL'ISTITUTO COMPRENSIVO DI SAN PAOLO D'ARGON
PROF. VINCENZO DEMICHELE

Visto l'art. 29 del D.Lgs. 196/2003 e successive modifiche ed integrazione,

NOMINA

in qualità di Responsabili del trattamento dei dati personali con responsabilità' di coordinamento e supervisione

la DSGA Francioni Giovanna

alla quale sono assegnate le seguenti responsabilità:

- svolgere attività di coordinamento e supervisione nei confronti degli altri responsabili del trattamento dei dati;
- verificare e monitorare il processo di adozione e messa in atto delle misure di sicurezza previste dal DPS - Documento Programmatico di Sicurezza, documentando e segnalando eventuali situazioni di ritardo e inadempienza;
- fornire, laddove richiesto, supporto metodologico ed organizzativo in merito alle questioni riguardanti la privacy e la sicurezza , soprattutto in fase di prima applicazione delle norme previste dal D.Lgs. 196/2003.

San Paolo d'Argon, ……..

Il Direttore Amministrativo
Francioni Giovanna

Il Dirigente Scolastico
Prof. Vincenzo Demichele

Allegato 4: Atto del Dirigente Scolastico di nomina dell'Amministratore di Sistema

Prot.n. ……/A20s del ……..

ATTO DI NOMINA DELL'AMMINISTRATORE DI SISTEMA -DISCIPLINARE TECNICO IN MATERIA DI MISURE MINIME DI SICUREZZA)

Il DIRIGENTE SCOLASTICO DELL'ISTITUTO COMPRENSIVO DI SAN PAOLO D'ARGON
PROF. VINCENZO DEMICHELE

Visto il comma 19. del Disciplinare Tecnico, che prevede "la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati";

NOMINA

il Signor _____ - Ass.te Amm.vo

Amministratore di Sistema

I compiti affidati all'Amministratore di Sistema sono analiticamente specificati per iscritto nella sezione 2 Istruzioni per l'Amministratore di Sistema" del Documento Programmatico sulla Sicurezza, custodito a cura della Segreteria Generale, di cui si riporta un estratto:

(inizio estratto:)

L'Amministratore di Sistema deve attenersi scrupolosamente alle seguenti istruzioni:

1. rispettare e mettere in atto le misure di sicurezza riportate nel DPS e quelle previste da leggi e norme vigenti in materia; più in generale, assicurare che l'utilizzo delle risorse informatiche e telematiche e delle banche dati elettroniche dell'Istituto avvenga con un adeguato livello di sicurezza e privacy;
2. assumere il compito di gestire in maniera sistematica e tempestiva il ciclo di vita dei profili e dei meccanismi di accesso degli Incaricati: generazione di user-id, password, profili di accesso etc; loro modifica, sospensione e evoca; fare in modo che dopo sei mesi di mancato utilizzo, gli account siano disattivati e non cancellati, non riutilizzare, nemmeno in tempi diversi, il medesimo user-id; verificare e assicurare che le password siano modificate ogni sei mesi, e nel caso di dati sensibili, siano modificate ogni tre mesi,
3. assicurare il salvataggio dei dati centralizzati con cadenza almeno quotidiana, e la possibilità di ripristinarli interamente e correttamente; verificare quotidianamente il corretto avvenuto salvataggio dei dati, e riporre le casette (e in generale i supporti utilizzati per la produzione delle copie di sicurezza, di qualsiasi tipo essi siano) in apposito armadio ignifugo dotato di serratura e chiave funzionante, oppure consegnarle alla Segreteria Generale che provvedere a riporle nella cassaforte dell'Ufficio Economato oppure presso una cassetta di sicurezza in banca;
4. individuare, formalizzare e mettere in atto adeguati piani e procedure di Disaster recovery e Business Continuity,, secondo quanto prescritto dall'Art. 4 punto f) del D.Lgs. 196/2003:
5. collaborare con il Titolare nel richiedere ai fornitori esterni di rilasciare una dichiarazione scritta di conformità dei nuovi software e/o hardware ai requisiti del Disciplinare Tecnico; in caso di non conformità o renitenza da parte del fornitore, vietare tassativamente l'installazione di nuovo software e/o hardware e darne immediata comunicazione al Dirigente Scolastico;
6. identificare, segnalare ed eliminare casistiche di utilizzo non strettamente personale di user-id e password;
7. identificare e segnalare al Titolare e ai Responsabili del trattamento dei dati casistiche di utilizzo non conforme al DPS, alla normativa vigente, e comunque non corrette e ortodosse, delle risorse informatiche e telematiche dell'Istituto;
8. assicurare la possibilità di accedere tempestivamente ai dati in situazioni di emergenza, secondo quanto prescritto dall'art. 10 del Disciplinare Tecnico del D.Lgs. 196/2003; a tale scopo è tenuto a consegnare al Custode delle Password un documento in formato cartaceo contenente l'elenco delle User ID e delle password associate a tutti i profili di tipo " Administrator" relativamente a tutti gli applicativi centralizzati e ai sistemi operativi utilizzati, nonché a tutti gli apparati di sicurezza e connettività gestiti (firewall, router, switch, dispositivi di accesso remoto, etc.);
9. adottare programmi antivirus, firewall ed altri strumenti, sia software che hardware, che possano garantire - anche in relazione alle conoscenze tecnologiche acquisite in base al progresso tecnico - la sicurezza nel trattamento dei dati personali, una adeguata protezione perimetrale e un adeguato livello di protezione contro virus e codici maligni;
10. assumere l'obbligo di eseguire periodicamente i controlli (avvalendosi eventualmente di collaboratori, consulenti e società specializzate che possono assicurare la completezza e l'accuratezza dei controlli) per verificare regolarmente l'efficienza e la validità delle misure di sicurezza adottate, con cadenza almeno semestrale; a valle dei controlli effettuati, è necessario aggiornare il DPS nelle sezioni di pertinenza;
11. monitorare, anche su richiesta del responsabile del trattamento dei dati, l'utilizzo della posta elettronica e di Internet, al fine

di evidenziare utilizzi non corretti;

12. assumere il compito di individuare e rimuovere periodicamente (almeno ogni sei mesi) la presenza di vulnerabilità applicative e sistemistiche presenti negli applicativi gestionali, nel web server, nel mail server, nei firewall, nei router, negli switch e nei server applicativi dell'Istituto, che possono compromettere, anche parzialmente, la sicurezza e l'operatività dei programmi applicativi gestiti centralmente. Nell'effettuare i controlli e le verifiche di cui sopra, ha la facoltà di avvalersi di collaboratori, consulenti e società speciali possono assicurare la completezza l'accuratezza dei controlli richiesti;
13. fornire supporto al Responsabile del trattamento dei dati, nell'individuare le modalità e le procedure di reimpiego dei supporti di memorizzazione di tipo fisso (come ad esempio i dischi rigidi), ex. Art. 21 e 22 del disciplinare Tecnico del D.Lgs. 196/2003 e, se del caso, definire gli strumenti e le procedure adeguate per procedere alla distruzione e smaltimento dei supporti di memorizzazione di tipo fisso che non possono essere riutilizzati.

(fine estratto)

In caso di aggiornamenti, integrazioni e modifiche del Documento Programmatico sulla Sicurezza, sarà cura della Segreteria Generale comunicare una nuova versione del Documento Programmatico sulla Sicurezza - oppure la parte modificata - all'Amministratore di Sistema.
In fase di prima adozione della normativa, l'Amministratore di Sistema potrà chiedere supporto metodologico e procedurale alla Segreteria Generale.

Il presente provvedimento ha decorrenza dalla data di notifica dello stesso agli interessati.

San Paolo d'Argon, lì ……..

Il Dirigente Scolastico
Prof. Vincenzo Demichele

Allegato 5 - Atto di nomina da parte del Dirigente Scolastico del Custode delle Parole Chiave dei Laboratori

Prot.n. ……/A20s del……..

ATTO DI NOMINA DEL CUSTODE DELLE PAROLE CHIAVE DEI LABORATORI

Il DIRIGENTE SCOLASTICO DELL'ISTITUTO COMPRENSIVO DI SAN PAOLO D'ARGON
PROF. VINCENZO DEMICHELE

Visto il comma 19.2 del Disciplinare Tecnico, che prevede 2la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati",

NOMINA

il Signor ----------

Custode delle Parole Chiave dei Laboratori.

I compiti affidati al Custode delle Parole Chiave dei Laboratori sono analiticamente specificati per iscritto nella sezione "Istruzioni per il Custode delle Parole Chiave dei Laboratori " Documento Programmatico sulla sicurezza, custodito a cura della Segreteria Generale, di cui si riporta un estratto:

(inizio estratto:)

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

1. custodire all'interno di una busta sigillata, datata e firmata sul lato esterno, l'elenco dei codici identificativi personali e delle corrispondenti parole chiave, relative a tutti i Personal Computer e i Server presenti nei Laboratori di Informatica (e in eventuali altri Laboratori) dell'Istituto; questo elenco dovrà comprendere inoltre anche i codici identificativi personali e le parole chiave relative ai router, ai firewall, agli switch, e i n generale a tutti gli apparati di sicurezza e di connettività gestititi dall'Istituto;
2. depositare la suddetta presso la cassaforte della Segreteria Generale oppure in una cassetta di sicurezza presso una Banca indicata dal Dirigente Scolastico;
3. dare indicazioni ad eventuali Software House o fornitori esterni affinché, in caso di modifica o creazione o di una nuova parola chiave, sia data contestuale comunicazione al Custode delle Parole Chiave dei Laboratori secondo la prassi indicata al punto 1;
4. per quanto riguarda le parole chiave utilizzate anche da Software House o fornitori esterni, a campione, e con una certa frequenza, aprire il contenuto delle buste e verificare che le password contenute siano effettivamente quelle in uso, in caso di inadempienza darne immediata comunicazione al Dirigente Scolastico.
5. in caso di comprovata necessità, dovrà recuperare le buste contenenti le parole chiave di sistema dalla cassaforte dell'Ufficio Segreteria oppure dalla cassetta di sicurezza presso la banca indicata dal Dirigente Scolastico, e utilizzare le parole chiave per assicurare la disponibilità dei dati e delle applicazioni, dandone contestuale notifica al dirigente Scolastico,

(fine estratto)

In caso di aggiornamenti, integrazioni e modifiche del Documento Programmatico sulla Sicurezza, sarà cura della Segreteria Generale comunicare una nuova versione del Documento Programmatico sulla Sicurezza - oppure la parte modificata - al Custode delle Parole Chiave dei Laboratori.

In fase di prima adozione della normativa, il Custode delle Parole Chiave dei Laboratori potrà chiedere supporto metodologico e procedurale alla Segreteria Generale.

II presente provvedimento ha decorrenza immediata.

San Paolo d'Argon, lì ……..

Il Custode delle Parole Chiave dei Laboratori

Il Dirigente Scolastico
Prof. Vincenzo Demichele

Allegato 6: Atto del Dirigente Scolastico di nomina del Custode delle Parole Chiave di Sistema

Prot.n. ……../A20s del ……

ATTO DI NOMINA DEL CUSTODE DELLE PAROLE CHIAVE DI SISTEMA (Art. 19 DELL'ALLEGATO B AL D.LGS. 196/20033: DISCIPLINARE TECNICO IN AMTERIA DI MISURE MINIME DI SICUREZZA)

Il DIRIGENTE SCOLASTICO DELL'ISTITUTO COMPRENSIVO DI SAN PAOLO D'ARGON
PROF. VINCENZO DEMICHELE

Visto il comma 19.2 del Disciplinare Tecnico, che prevede "la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati";

NOMINA

il DSGA Francioni Giovanna

Custode delle Parole Chiave di Sistema

I compiti affidati al Custode delle Parole Chiave di Sistema sono analiticamente specificati per iscritto nella sezione "Istruzioni per il Custode delle Parole Chiave - Parole Chiave di Sistema " del Documento Programmatico sulla Sicurezza, custodito a cura della Segreteria Generale, di cui si riporta un estratto:
(inizio estratto:)

II Custode delle Parole Chiave di Sistema deve attenersi scrupolosamente alle seguenti istruzioni:

1. richiedere e ottenere, con cadenza almeno semestrale, all'Amministratore di Sistema, una busta chiusa e sigillata, datata e firmata sul lato esterno, contenente l'elenco dei codici identificativi personali e delle corrispondenti parole chiave, relative ai profili per la gestione del sistema utilizzati per l'accesso a livello sistematico e applicativo; questo elenco dovrà comprendere inoltre anche i codici identificativi personali e le parole chiave relative ai router, ai firewall, agli switch, e in generale a tutti gli apparati di sicurezza e di connettività gestiti dall'Istituto;
2. depositare la suddetta presso la cassaforte della Segreteria generale oppure in una cassetta di sicurezza presso una Banca indicata dal Dirigente Scolastico;
3. dare indicazioni all'Amministratore di Sistema affinché, in caso di modifica o creazione di una nuova parola chiave, sia data contestuale notifica al custode della Parole Chiave di Sistema secondo la prassi indicata al punto 1;
4. a campione, e con una certa frequenza , aprire il contenuto delle buste ottenute dall'Amministratore di Sistema e verificare che le password contenute siano effettivamente quelle in uso; dopo aver effettuato la verifica, darne notifica all'Amministratore di Sistema, che provvedere alla modifica della password sottoposta a verifica;
5. in caso di comprovata necessità, dovrà recuperare le buste contenenti le parole chiave di sistema dalla cassaforte dell'Ufficio Segreteria oppure dalla cassetta di sicurezza presso la banca, e utilizzare le parole chiave per assicurare la disponibilità dei dati e delle applicazioni, dandone contestuale notifica al Titolare del trattamento dei dati.

(fine estratto)

In caso di aggiornamenti, integrazioni e modifiche del Documento programmatico sulla Sicurezza, sarà cura della Segreteria Generale comunicare una nuova versione del Documento Programmatico sulla Sicurezza - oppure la parte modificata - all'Amministratore di Sistema.
In fase di prima adozione della normativa, il Custode della parola Chiave di Sistema potrà chiedere supporto metodologico e procedurale alla Segreteria Generale.

Il presente provvedimento ha decorrenza dalla data di notifica dello stesso agli interessati.

San Paolo d'Argon,

Il Custode delle Parole Chiave di Sistema:

Francioni Giovanna

Il Dirigente Scolastico
Prof. Vincenzo Demichele

Prot.n. ……./A20s del…….

Allegato 7: Atto di nomina ad Incaricato del trattamento dei dati (opzionale)

Nota: l'instanzazione del presente atto è opzionale, in quanto - per come è stato strutturato il documento "NOMINA AD INCARICATO e REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI" - la consegna del documento stesso, e la firma da parte del Responsabile e dell'incaricato, costituiscono a tutti gli effetti una modalità di designazione e nomina dell'incaricato del trattamento dei dati.

20. Allegato 6: Atto del Dirigente Scolastico di nomina del Custode delle Parole Chiave di Sistema
ATTO DI NOMINA AD INCARICATO DEL TRATTAMENTO DEI DATI (art. 30 DEL D.LGS. 196/2003 - CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI)

La sottoscritta FRANCIONI GIOVANNA

In qualità di responsabile del trattamento dei dati con responsabilità di coordinamento e supervisione,
Visto l'art. 30 del D.Lgs. 196/2003, che prevede l'obbligo di designare gli incaricati del trattamento dei dati, individuando puntualmente l'ambito del trattamento consentito;

- Visto il comma 19.2 del Disciplinare Tecnico, che prevede la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati",
-

NOMINA

In qualità di Incaricato del trattamento dei dati all'interno dell'Area summenzionata il Signor/la Signora:

L'incaricato del trattamento dei dati è tenuto, ai sensi dell'art. 30 del DLgs. 196/2003, a rispettare scrupolosamente il contenuto del documento "NOMINA AD INCARICATO E REGOLAMENTO PER IL TRATTAMENTO DEI DATI PERSONALI", allegato al presente atto

San Paolo d'Argon, ……

Il Titolare o responsabile del trattamento dei dati:

L'Incaricato del trattamento dei dati

Il Direttore Amm.vo
Francioni Giovanna