MINISTERO DELL'ISTRUZIONE E DEL MERITO
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
I.C. "PIAZZA FILATTIERA 84"
Piazza Filattiera, 84 - 00139 ROMA - Tel. 06/8102978
C.M. RMIC8EG00Q – C.F. 97713420582
e-mail: rmic8eg00q@istruzione.it pec: rmic8eg00q@pec.istruzione.it

MODELLO ORGANIZZATIVO PRIVACY

LE ATTIVITA' DI TRATTAMENTO DEI DATI PERSONALI

(Art. 30 Regolamento UE 2016/679)

IL DATA PROTECTION IMPACT ASSESSMENT

(art. 35 del REGOLAMENTO EUROPEO 679/2016)

Figura da EPS

IL TITOLARE DEL TRATTAMENTO ***IL DATA PROTECTION OFFICIER***

Prof. Claudio Finelli Dott. Giuseppe Renato Croce

SOMMARIO

PARTE TERZA

CONCLUSIONI DERIVANTI DALL'ANALISI DEI RISCHI

PARTE QUARTA

GLI ALLEGATI

ALLEGATO n°8: LE TABELLE

TABELLA 1 Connettività internet
TABELLA 2 Descrizione Personal Computer

GENERALITA'

A1. I DATI IDENTIFICATIVI DELLA ISTITUZIONE SCOLASTICA

Istituto Comprensivo Statale "Piazza Filattiera 84", Roma – RMIC8EG00Q

RAPPRESENTANTE LEGALE PRO TEMPORE TITOLARE DEL TRATTAMENTO:

Prof. Claudio Finelli
C.F. FNLCLD73B27F839W
TEL. 068102978
e-mail rmic8eg00q@istruzione.it
posta certificata: rmic8eg00q@pec.istruzione.it

Docenti: 163

Alunni: n.1266

Ass. Amministrativo: n. 6

Ass. Tecnici: 0

Collaboratori scol.: n.21

RESPONSABILE DELLA PROTEZIONE DATI (RPD)
tipo di designazione: esterno
Dati Responsabile: Dr. Giuseppe Renato Croce
P.IVA: 12946091001
posta certificata: giusepperenato.croce@pec.it

RESPONSABILE INTERNO DEL TRATTAMENTO: prof. C. Finelli

A2. I PRINCIPI FONDAMENTALI DEL TRATTAMENTO DI DATI

L'art. 5 del GDPR 2016/679 stabilisce che ogni trattamento di dati personali deve avvenire nel rispetto dei seguenti principi:

- **Liceità**: i dati devono essere trattati in modo lecito, corretto e trasparente;
- **limitazione della finalità**: i dati devono essere raccolti per finalità legittime ed individuate fin dall'inizio, e successivamente trattati in modo che non sia incompatibile con tali finalità. Unica eccezione a questo principio è l'ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici;
- **minimizzazione dei dati**: i dati trattati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- **esattezza**, nel senso che devono essere corretti e, se necessario, aggiornati, con conseguente obbligo di cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati;
- **limitazione della conservazione**: è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento. È ammessa una conservazione più lunga a condizione che siano trattati esclusivamente per finalità di archiviazione nel pubblico interesse, di ricerca scientifica o storica e statistica;
- **integrità e riservatezza**: i dati sono trattati in maniera da garantire un'adeguata sicurezza, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

Il Titolare del Trattamento oltre che osservare questi principi deve essere in grado, altresì, di dimostrare di avere messo in atto misure tecniche e organizzative adeguate per garantire,, che il trattamento è effettuato conformemente al GDPR e deve essere "in grado di comprovarlo". (principio di "***responsabilizzazione" o accountability***)

A3. LA MISSION DELLA ISTITUZIONE SCOLASTICA

L'Istituzione Scolastica I.C. Piazza Filattiera 84, nell'ambito della propria funzione istituzionale tratta ordinariamente **DATI PERSONALI COMUNI e DATI PERSONALI PARTICOLARI** (quali previsti negli artt. 9 e 10 Reg Europeo 679/2016) di studenti, personale scolastico e terzi per realizzare la seguente *mission*:

- Garanzia del servizio scolastico
- Gestione e formazione del personale
- Certificazione degli esiti scolastici e dei servizi prestati dai dipendenti
- Acquisizione di beni e servizi da terzi fornitori
- Attività strumentali alle precedenti
- Adempimenti assicurativi

E' previsto che queste finalità vengano raggiunte in osservanza del principio detto di "***responsabilizzazione" (o accountability***)" quale affermato nell'art. 5 par.2 del GDPR 679/2016:a tal fine ogni trattamento di dati personali è previsto che avvenga nel rispetto dei principi che in sintesi riguardano:

- liceità, correttezza e trasparenza del trattamento, nei confronti dell'interessato;
- limitazione della finalità del trattamento, compreso l'obbligo di assicurare che eventuali trattamenti successivi non siano incompatibili con le finalità della raccolta dei dati;
- minimizzazione dei dati: ossia, i dati devono essere adeguati pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento;
- esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento;
- limitazione della conservazione: ossia, è necessario provvedere alla conservazione dei dati per un tempo non superiore a quello necessario rispetto agli scopi per i quali è stato effettuato il trattamento;
- integrità e riservatezza: occorre garantire la sicurezza adeguata dei dati personali.

A4. LE BANCHE DATI E I DATI PERSONALI COMUNI E PARTICOLARI

Alla stregua, quindi, l'Istituzione Scolastica, ha formato delle **BANCHE DATI** che contengono i menzionati **DATI COMUNI** e **DATI PARTICOLARI** che vengono trattati esclusivamente presso gli Uffici dell'Istituto o piattaforma di gestione documentale messa a disposizione da un fornitore esterno(in questo caso è stato nominato un Responsabile esterno del trattamento). E' previsto che i dati potranno essere comunicati a terzi solo nell'ambito dell'attività istituzionale dell'Istituto e comunque nei casi previsti dalla informativa fornita agli interessati ed in seguito ad esplicito consenso espresso dagli stessi.

Le BANCHE DATI contengono i Dati Personali dei seguenti interessati:

- ***Alunni:***

a. Documenti riguardanti gli alunni, relativi al corso di studi, alla presenza di handicap, alla certificazione dell'idoneità alla pratica sportiva non agonistica, alla scelta dell'insegnamento della religione cattolica, all'esito di scrutini, esami, piani educativi individualizzati differenziati
b. Documenti prodotti dalle famiglie riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche.
c. Altri Rapporti scuola – famiglie
d. Organismi collegiali e commissioni istituzionali

- ***Dipendenti:***

a. Documentazione riguardante il personale docente e non docente, con elementi di individuazione di appartenenza sindacale, stato di salute, anche di congiunti per i quali vengono richiesti benefici previsti da particolari norme, allo stato di servizio, alla retribuzione, alle eventuali pratiche disciplinari.
b. Gestione del contenzioso e procedimenti disciplinari

- ***Protocollo***
- ***Inventario***
- ***Magazzino***
- ***Rapporti con enti ed imprese***
- ***Fornitori***
- ***Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi***
- ***Contabilità e Bilancio***

I DATI PERSONALI COMUNI E PARTICOLARI

I DATI PERSONALI trattati si distinguono in:

- **DATI COMUNI:**

a. dati comuni degli studenti maggiorenni, degli studenti minorenni, degli esercenti la responsabilità genitoriale ;
b. dati comuni del personale scolastico (Docenti e personale A.T.A.) funzionali al rapporto di lavoro, alla reperibilità alla corrispondenza con gli stessi o richiesti a fini fiscali e previdenziali.
c. dati comuni di consulenti, esperti, ecc. dagli stessi comunicati per l'espletamento dell'incarico professionale, compresi dati sul patrimonio e sulla situazione economica, o necessari a fini fiscali o attinenti alla reperibilità e alla corrispondenza con gli stessi.

d. dati comuni dei fornitori forniti dagli stessi e relativi alla reperibilità o alla corrispondenza con gli stessi nonché inerenti a fini fiscali o di natura bancaria.
e. dati comuni forniti da altre Istituzioni Scolastiche o MIUR ,USR

- **<u>DATI PARTICOLARI</u> indicati negli artt.9 e 10 del Regolamento UE n.679/2016 in coerenza col D.Lvo 101/2018:**

a. dati del personale dipendente conseguenti al rapporto di lavoro, ovvero inerenti i rapporti con gli enti previdenziali ed assicurativi e assistenziali, o dati giudiziari del personale dipendente o l'adesione ad organizzazioni sindacali.
b. dati forniti dagli interessati idonei a rivelare l'origine razziale ed etnica le convinzioni o l'adesione ad organizzazioni a carattere religioso politico ,sindacale, filosofico
c. dati forniti dagli interessati o acquisiti per l'espletamento delle funzioni istituzionale idonei a rivelare lo stato di salute.
d. categorie particolari di dati personali relativi a condanne penali e reati

PRIMA PARTE

LE ATTIVITA' DI TRATTAMENTO DEI DATI PERSONALI

A. IL REGISTRO DELLE ATTIVITA' DI TRATTAMENTO DATI PERSONALI

(art. 30 del GDPR 2016/679)

(Per la realizzazione del Registro delle Attività di Trattamento si è, anche, tenuto conto della nota prot. MIUR n. 563 del 22/05/2018 e della relativa Guida alla compilazione del Registro delle attività di trattamento inviata sempre dal MIUR alle Istituzioni Scolastiche nel luglio 2018.)

Il Registro delle Attivita' di Trattamento Dati Personali, in riferimento al funzionigramma e alle categorie di Dati Personali quali esplicitati nel Capo A. è una rappresentazione (in forma digitale) delle modalità in uso nell'Istituto Scolastico avente lo scopo di informare, dare consapevolezza e condivisione del processo di gestione del ***DATO PERSONALE*** e riporta le seguenti informazioni:

- dati di contatto del titolare del trattamento e dei contitolari del trattamento e del Responsabile della protezione dei dati;
- le finalità per le quali sono trattati tali dati;
- categorie di interessati;
- categorie di dati personali;
- categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- una descrizione generale delle misure di sicurezza tecniche e organizzative.

IL REGISTRO, in forma digitale (*template*) e composto da **diciotto sezioni** così denominate :

- **CATEGORIE DEGLI INTERESSATI**
- **LE ATTIVITÀ OGGETTO DEL TRATTAMENTO**

- **DESCRIZIONE DELLE ATTIVITÀ DEL TRATTAMENTO**
- **MODALITÀ DEL TRATTAMENTO**
- **FINALITÀ DEL TRATTAMENTO**
- **TIPOLOGIA DEL TRATTAMENTO**
- **BASE GIURIDICA DEL TRATTAMENTO**
- **INFORMATIVA**
- **DATI COMUNI**
- **CATEGORIE PARTICOLARI DI DATI PERSONALI**
- **CATEGORIE**
- **TERMINI DI CANCELLAZIONE**
- **DESTINATARI ESTERNI DEI DATI**
- **TRASFERIMENTO ALL'ESTERO DEI DATI**
- **PAESI EXTRA UE O ORGANIZZAZIONI INTERNAZIONALI VERSO I QUALI VENGONO TRASFERI I DATI**
- **MISURE DI SICUREZZA**
- **CONTITOLARE DEL TRATTAMENTO**
- **RESPONSABILE ESTERNO DEI DATI**

1. CATEGORIE DEGLI INTERESSATI

In questa Sezione sono indicate le categorie di interessati al trattamento di dati personali, che presso l'Istituzione Scolastica, si identificano in:

- Alunni
- Esercenti la responsabilità genitoriale
- Personale Docente
- Personale ATA
- Responsabile del Servizio di Prevenzione e Protezione
- Altro personale utilizzato
- Rappresentanti di organizzazioni sindacali
- Rappresentanti e dipendenti di operatori economici
- Delegati di soggetti privati
- Professionisti, intermediari
- Visitatori
- Altri soggetti - Persone fisiche

2. LE ATTIVITÀ OGGETTO DEL TRATTAMENTO

In questa Sezione sono riportate i tipi di attività effettuate dall'Istituzione scolastica, soggette a procedure aventi la medesima modalità di trattamento, finalità, tipologia di trattamento, base giuridica e categoria di interessati

3. DESCRIZIONE DELLE ATTIVITÀ DEL TRATTAMENTO

In questa Sezione è riportata la descrizione sintetica dell'attività nell'ambito della quale vengono trattati i dati personali.

4. MODALITÀ DEL TRATTAMENTO

In questa Sezione sono indicati i mezzi e gli strumenti attraverso i quali viene effettuato il trattamento e specificatamente:

- Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici);
- Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc., presenti su una postazione di lavoro);
- Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)

Nella sezione apposita vengono riportate, nello specifico, le modalità di conservazione e trattamento dei Dati.

5. FINALITÀ DEL TRATTAMENTO

In questa Sezione è indicato lo scopo determinato, esplicito e legittimo, perseguito nell'ambito dell'attività di trattamento di dati personali nel rispetto dei principi sanciti nell' art. 5 del GDPR 679/2016

6. TIPOLOGIA DEL TRATTAMENTO

In questa Sezione sono riportate le operazioni materialmente effettuata sui dati trattati. Le tipologie di trattamento sono la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione dei Dati".

7. BASE GIURIDICA DEL TRATTAMENTO

In questa Sezione sono riportate le condizioni che rendono lecito il trattamento di dati

che sono:
- Consenso dell'interessato
- Esecuzione di un contratto con l'interessato o esecuzione di misure precontrattuali adottate su richiesta dello stesso
- Obbligo legale per il titolare
- Salvaguardia interessi vitali dell'interessato o altra persona fisica
- Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da normativa nazionale
- Esecuzione di un compito di interesse pubblico o pubblici poteri del titolare derivante da regolamento UE
- Altri fondamenti connessi al trattamento di categorie particolari di dati personali - art. 9 par. 2 del Regolamento
- Legittimo interesse

8. INFORMATIVA

In questa Sezione viene indicata se è necessaria un'informativa sul trattamento dei dati personali.
Le opzioni su "Informativa" sono:

- Sì, Informativa ex art. 13 del Regolamento UE 679/2016 (Dati raccolti presso l'interessato);
- Sì, Informativa ex art. 14 del Regolamento UE 679/2016 (Dati ottenuti da soggetto diverso dall'interessato);
- No

9. DATI COMUNI

In questa Sezione sono raccolte le informazioni raccolte che consentono di identificare una persona fisica.
I dati comuni sono:
Dati anagrafici

- Dati contabili, fiscali e finanziari
- Dati inerenti il rapporto di lavoro
- Dati derivanti da tracciamenti (log)
- Dati inerenti situazioni giudiziarie civili, amministrative, tributarie
- Dati che consentono la geolocalizzazione
- Dati audio/foto/video
- Dati di profilazione

10. CATEGORIE PARTICOLARI DI DATI PERSONALI

In questa Sezione sono indicati i dati personali idonei a rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona.

11. DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI

In questa Sezione sono indicati i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'art. 6, paragrafo 1 del Regolamento UE 679/2016.
I dati personali relativi a condanne penali e reati sono:

- Iscrizione nel casellario giudiziale
- Condizione di indagato/imputato o altre situazioni giudiziarie (condanne penali e reati o connesse misure di sicurezza)
- Sottoposizione a misure detentive carcerarie

12. TERMINI DI CANCELLAZIONE

In questa Sezione sono indicati i termini di cancellazione dei dati personali trattati.

13. DESTINATARI ESTERNI DEI DATI

In questa Sezione sono indicati i soggetti cui possono essere comunicati da parte del titolare. i dati personali trattati al fine di specificare il flusso di informazioni dal titolare verso l'esterno.
I destinatari esterni dei dati sono:

- Pubblica Amministrazione
- Soggetti privati (persone fisiche o giuridiche)

14. TRASFERIMENTO ALL'ESTERO DEI DATI

In questa Sezione sono indicate le condizioni che autorizzano qualunque trasferimento di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento verso un paese terzo o un'organizzazione internazionale, compresi trasferimenti successivi di dati personali da un paese terzo o un'organizzazione internazionale verso un altro paese terzo o un'altra organizzazione internazionale.
Le condizioni che autorizzano il trasferimento all'estero sono:
- Trasferimento sulla base di una decisione di adeguatezza (art. 45 del Regolamento)
- Trasferimento soggetto a garanzie adeguate (art. 46 del Regolamento)

- Consenso dell'interessato al trasferimento
- Esecuzione di un contratto tra titolare e interessato
- Esecuzione di un contratto tra titolare e soggetto che agisce per conto dell'interessato
- Interesse pubblico
- Accertamento, esercizio o difesa di un diritto in sede giudiziaria
- Tutela degli interessi vitali dell'interessato o di terzi
- Predisposizione di un registro normato dal diritto dell'UE

15. PAESI EXTRA UE O ORGANIZZAZIONI INTERNAZIONALI VERSO I QUALI VENGONO TRASFERI I DATI

In questa Sezione è indicata la denominazione del paese extra-UE o dell'organizzazione internazionale verso i quali sono trasferiti i dati personali

16. MISURE DI SICUREZZA

In questa Sezione sono indicate le misure di sicurezza organizzative e tecniche adottate per ridurre al minimo i rischi di distruzione o perdita dei dati, accesso non autorizzato, trattamento non consentito e modifica dei dati personali trattati. Le misure di sicurezza sono:

- Minimizzazione della quantità di dati personali
- Cifratura
- Pseudonomizzazione
- Cancellazione sicura
- Controllo degli accessi logici ed autenticazione
- Sicurezza dell'ambiente operativo
- Sicurezza della rete e delle comunicazioni
- Tracciatura e monitoraggio
- Gestione sicura dell'hardware, delle risorse e dei dispositivi
- Gestione sicura delle postazioni di lavoro
- Backup e Continuità operativa
- Manutenzione delle apparecchiature
- Protezione delle fonti di rischio ambientali
- Politiche e procedure per la protezione dei dati personali
- Gestione dei Responsabili del trattamento e delle terze parti
- Sicurezza del ciclo di vita delle applicazioni e nei progetti
- Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali
- Gestione e formazione del personale
- Controllo degli accessi fisici
- Sicurezza dei documenti cartacei

17. CONTITOLARE DEL TRATTAMENTO

In questa Sezione è indicato il nome del contitolare del trattamento quando due o più soggetti determinano congiuntamente le finalità e i mezzi del trattamento (es. MIUR,USR)

18. RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI

In questa Sezione è indicato il nome del responsabile esterno del trattamento: la persona fisica o giuridica che tratta dati personali per conto del titolare del trattamento.

B. CATEGORIE DI DATI E RESPONSABILITA' FUNZIONALI

CATEGORIE DI DATI PERSONALI TRATTATI		**RESPONSABILITA' FUNZIONALE**	**MODALITA' DEL TRATTAMENTO**
CAT. A	**Selezione, reclutamento, gestione del rapporto di lavoro del personale dipendente, ivi ricompresi i dati personali particolari ex artt. 9 e 10 Reg. Europeo 679/2016 (relativi a condanne civili e penali, e dati relativi alla salute).** **Nello Specifico:** Fascicoli del personale ATA Fascicoli del personale docente Contratti per supplenze Gestione organico (graduatorie, trasferimenti, ecc.) Fascicoli supplenti Visite collegiali e fiscali Assenze e permessi Fascicoli Ricostruzione di carriera Gestione del contenzioso e procedimenti disciplinari Dipendenti e Assimilati	Dirigente Scolastico, DSGA e sub responsabili del trattamento/ incaricati (personale amministrativo e assimilati, Collaboratori del D.S., Medico Competente qualora nominato)	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)
CAT. B	**Organismi collegiali e commissioni istituzionali**. **Nello specifico:** la documentazione degli Organi collegiali (Verbali di assemblea, convocazioni, provvedimenti, ecc.) e comunicazioni di vario tipo per la gestione dei rapporti sindacali con le RSU	Dirigente Scolastico, DSGA e sub responsabili del trattamento/ incaricati (personale amministrativo e assimilati, Collaboratori del D.S.)	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)

CAT. C	**Attività di gestione economica e finanziaria.** **Nello specifico:** Inventario; Magazzino; Rapporti con enti ed imprese; Fornitori ; Dati per gestire le negoziazioni e le relative modalità di pagamento per la fornitura di beni e servizi; Gestione archivi elettronici della contabilità; Gestione retribuzioni e documenti contabili e fiscali del personale Dichiarazioni per finalità assistenziali, previdenziali e pensionistici; Gestione documentazione ore di servizio Gestione rapporti con i fornitori; Gestione programma annuale e Fondo di istituto; Corretta tenuta dei registri contabili previsti dal D.M. n. 129/2018 e correlata normativa vigente.	Dirigente Scolastico, DSGA e sub responsabili del trattamento/ incaricati (personale amministrativo e assimilati, Collaboratori del D.S.)	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)
CAT. D	**Attività propedeutiche all'avvio dell'anno scolastico.** **Nello specifico**: Fascicoli degli alunni Fascicoli riservati alunni con disabilità Documentazione propedeutica all'avvio dell'anno scolastico (iscrizione, classi, graduatorie, trasferimenti, ecc.) Documenti necessari per assicurazione e denuncia infortuni Procedimenti relativi alla frequenza (prolungamento orario, organizzazione servizio mensa ecc.); Archivio generale storico	Dirigente Scolastico, DSGA e sub responsabili del trattamento/ incaricati (personale amministrativo e assimilati Collaboratori del D.S.)	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)

CAT. E	**<u>Attività educative formative didattiche e di valutazione</u>** **<u>Nello specifico</u>**: Documenti di varia natura connessi all'attività educativa, didattica, formativa e di valutazione (diplomi, prove di valutazione intermedie e finali, registri, verbali, piano individualizzato, presenza di handicap, certificazione dell'idoneità alla pratica sportiva non agonistica, scelta dell'insegnamento della religione cattolica, esito di scrutini, esami, piani educativi individualizzati differenziati ecc.); Procedure Invalsi; Organizzazione Viaggi d'istruzione e Visite didattiche; Convocazioni GLH;	Dirigente Scolastico, DSGA e sub responsabili del trattamento/ incaricati (personale amministrativo e assimilati, Docenti, Collaboratori del D.S.)	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)
CAT. F	**<u>Rapporti scuola-famiglia compresa la gestione del contenzioso.</u>** **<u>Nello specifico</u>**: Documenti e comunicazioni di vario tipo relativi a: informazioni riservate, provvedimenti disciplinari e vicende giuridiche in corso e contenziosi; Documenti prodotti dalle famiglie riguardanti la certificazione della situazione patrimoniale e delle condizioni economiche; Altri Rapporti scuola – famiglie	Dirigente Scolastico, DSGA e sub responsabili del trattamento/ incaricati (personale amministrativo e assimilati, Docenti, Collaboratori del D.S.)	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)
CAT. G	**<u>Rapporti con: MIUR, altre Istituzioni scolastiche, Enti Locali, ASL e centri Handicap e sostegno di riabilitazione (trasmissione schede rilevazioni alunni H) e privati (Enti Privati e liberi professionisti</u>**). **<u>Nello specifico</u>**: Documenti e comunicazioni di vario tipo del protocollo e della posta elettronica dell'Istituto	Dirigente Scolastico, DSGA e sub responsabili del trattamento/ incaricati (personale amministrativo e assimilati, Collaboratori del D.S.)	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)
CAT: H	**<u>Gestione Istituzionale</u>**	Dirigente Scolastico, DSGA e Segreteria Amministrativa (e assimilati), Collaboratori del D.S.	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)

CAT.I	**<u>Gestione sito web dell'istituto</u>**	Dirigente Scolastico, Incaricati sito web (compresi incaricati esterni)	➢ Utilizzo di servizi ICT (il trattamento è effettuato attraverso l'utilizzo di applicativi informatici) ➢ Utilizzo di strumenti di office automation (il trattamento è effettuato utilizzando gli strumenti di Office, come Word, Excel, etc) ➢ Gestione Manuale (il trattamento è effettuato mediante l'utilizzo di supporti cartacei)

C. STRUTTURA ORGANIZZATIVA:COMPITI E RESPONSABILITA'

STRUTTURA ORGANIZZATIVA	TIPO DI DATO TRATTATO	COMPITI E RESPONSABILITA' DELLA STRUTTURA
TITOLARE DEL TRATTAMENTO Dirigente Scolastico	Dati comuni Dati particolari ex artt. 9 e 10 Reg. Europeo 679/216	Direzione generale di tutte le attività, gestione delle pratiche riservate
RESPONSABILE INTERNO DEL TRATTAMENTO: Direttore Servizi Generali Amm.vi	Dati comuni Dati particolari ex artt. 9 e 10 Reg. Europeo 679/216 e Specificatamente alla gestione amministrativo-contabile e alla gestione delle attività del personale ATA	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Collaboratori del DS	Dati comuni Dati particolari ex artt. 9 e 10 Reg. Europeo 679/216	Affiancamento al D.S. con deleghe parziali e sostituzione dello stesso in caso di assenza
Assistenti Amministrativi incaricati	Dati comuni Dati particolari ex artt. 9 e 10 Reg. Europeo 679/216 previa autorizzazione	Gestione amministrativa di tutte le pratiche e supporto al Dirigente Scolastico e al Corpo Docente
Docenti	Dati comuni In casi eccezionali Dati particolari ex artt. 9 e 10 Reg. Europeo 679/216	Insegnamento e attività integrative e collaterali, partecipazione alle scelte organizzative e di orientamento generale, partecipazione alla gestione di specifiche attività
Docenti Incaricati della redazione e gestione di Piani Educativi Individuali di alunni con handicap della creazione e gestione del sitowebe di tutti i trattamenti informatizzati e non relativi all'attività	Dati comuni Dati particolari ex artt. 9 Reg. Europeo 679/216 rigorosamente nei limiti relativi alle funzioni e previo consenso dell'avente diritto	attività propedeutiche all' avvio dell'anno scolastico e attività educativa, didattica e formativa e di valutazione
Docente o animatore Esterno	Dati comuni Dati particolari ex artt. 9 Reg. Europeo 679/216 rigorosamente nei limiti relativi alle funzioni e previo consenso dell'avente diritto	Attività di animazione a favore degli alunni della scuola

Collaboratori scolastici	Dati comuni ma con attività di supporto In casi eccezionali Dati particolari ex artt. 9 e 10 Reg. Europeo 679/216 con attività di supporto	Apertura e chiusura della sede, custodia e controllo, consegna e ricezione plichi e lettere, pulizia, assistenza a tutte le altre attività, gestione di dati comuni di alunni, docenti e familiari

Amministratore del sistema informatico	Tutti i trattamenti informatici, ma rigorosamente nei limiti della funzione	Gestione del sistema informatico dell'istituto
Custode delle passwords	Tutti i trattamenti informatici limitatamente alla funzione	Ogni Incaricato munito di accesso al computer mediante password, ad ogni scadenza della password (3 o 6 mesi, a seconda dei casi) consegna una busta chiusa contenente la password, da tenere a disposizione del Custode in caso di necessità di accesso agli archivi elettronici di quell'Incaricato quando è assente
Tecnico della Manutenzione del Software	Tutti i trattamenti, ma limitatamente alla funzione	Manutenzione del software e interventi sull'hardware
Incaricato Tecnico Esterno della Manutenzione dell'Hardware [se esistente]	tutti i trattamenti nei limiti relativi alle funzioni	Manutenzione dell'hardware dei computers
Personale incaricato della creazione e gestione del sito web	Dati comuni Dati particolari ex artt. 9 e 10 Reg. Europeo 679/216 in riferimento ai trattamenti informatici, rigorosamente nei limiti relativi alla gestione sito web dell'istituto	Creazione e gestione del sito web dell'Istituto Scolastico
Incaricato esterno per la creazione e gestione del sito web [se incaricato °]	i trattamenti informatici, rigorosamente nei limiti relativi alle seguenti attività: Gestione sito web dell'istituto	Creazione e gestione del sito web dell'Istituto
R.S.P.P. e Addetti al S.P.P., R.L.S.	I trattamenti relativi all'applicazione della normativa sulla sicurezza (Testo unico DLgs. 81/08 e normativa correlata)	Applicazione normativa Dlgs 81/2008 s.m.i. e norme collegate; gestione sicurezza sul posto di lavoro e nella scuola in generale
Medico competente ai sensi del Dlgs 81/2008 s.m.i.[se nominato]	I trattamenti relativi all'applicazione della normativa 81/2008 s.m.i. o ad essa riferiti: Trattamenti autorizzati: tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alla funzione	Applicazione normativa Dlgs 81/2008 s.m.i. e norme collegate; gestione sicurezza sul posto di lavoro

Responsabile Esterno del Trattamento : tipo AXIOS, SPAGGIARI e simili	Tutti i trattamenti informatici , ma rigorosamente nei limiti della funzione come da contratto di gestione (es: registro elettronico e simili)	organizzazione per la gestione manutenzione del Software e dell'Hardware come da clausole contrattuali
Responsabile Esterno del Trattamento : Agenzia di viaggio e simili e Gestori di trasporti	tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni:	Organizzazione di visite d'istruzione, visite didattiche, campi scuola e simili
Responsabile Esterno del Trattamento : Ente di certificazione di qualità [se esistente)	tutti i trattamenti informatici e non, rigorosamente nei limiti relativi alle funzioni	Verifica delle condizioni che consentono l'ottenimento del certificazione di qualità

19. LA MODULISTICA DI SUPPORTO

La Modulistica di Supporto, quale inviata ai Titolari del Trattamento dei Dati personali è la seguente:

- Designazione del Responsabile interno della trattazione dei dati personali;
- Designazione del Responsabile esterno della trattazione dei dati personali;
- Designazione del Responsabile esterno della trattazione dei dati personali in occasione di Viaggi d'istruzione o Visite didattiche;;
- Designazione dei Docenti quali incaricati del trattamento ;
- Nomina degli assistenti amministrativi ad incaricati/sub responsabili del trattamento dei dati personali;
- Nomina degli assistenti tecnici ad incaricati/sub responsabili del trattamento dei dati personali;
- Nomina dei collaboratori scolastici del trattamento dei dati personali;
- Informativa diretta agli esercenti la responsabilità genitoriale;
- Informativa diretta agli alunni maggiorenni;
- Informativa diretta al personale scolastico;
- informativa diretta ai fornitori;
- Nomina del Custode delle password
- Nomina Amministratore di Sistema

SECONDA PARTE

IL DATA PROTECTION IMPACT ASSESSMENT (DPIA)

(Art. 35 GDPR 679/2016)

GENERALITA'

Il **Data Protection Impact Assessment (DPIA)** è la Valutazione d'impatto che si deve effettuare per proteggere i dati personali, così come previsto dall'art. 35 del Regolamento Europeo n.2016/679 e consiste in un processo volto a descrivere i trattamenti, valutarne la necessità e la proporzionalità onde gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento.
Il soggetto obbligato ad effettuare un DPIA è il Titolare del trattamento con il supporto del DPO che deve monitorare lo svolgimento del DPIA e fornire il suo parere ai fini dell'esito positivo o meno del processo.
Il Regolamento Europeo per svolgere un processo di DPIA individua le seguenti fasi:

A) descrizione dei trattamenti previsti e delle finalità del trattamento:

- la natura, l'ambito di applicazione, il contesto e le finalità del trattamento;
- la registrazione dei dati personali, dei destinatari e dell periodo di conservazione dei dati personali;
- la descrizione funzionale del trattamento;
- le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei);

B) valutazione della necessità e proporzionalità dei trattamenti e determinazione delle misure di garanzia:

- misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
  - finalità determinate, esplicite e legittime;
  - liceità del trattamento;
  - dati personali adeguati, pertinenti e limitati a quanto necessario;
  - limitazione della conservazione;
  - misure che contribuiscono ai diritti degli interessati;
  - informazioni fornite all'interessato;
  - diritto di accesso e portabilità dei dati;
  - diritto di rettifica e alla cancellazione;
  - diritto di opposizione e di limitazione di trattamento;
  - rapporti con i responsabili del trattamento;

C) ***misure previste per dimostrare l'osservanza;***

D) ***valutazione dei rischi per i diritti e le libertà degli interessati:***

- origine, natura, particolarità e gravità dei rischi;
- fonti di rischio;
- individuazione degli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
- Individuazione delle minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati e stima delle probabilità di accadimento e della gravità;
- misure previste per gestire i rischi individuati.

E) ***misure previste per affrontare i rischi per cui vengono identificati:***

- gli impatti potenziali sui diritti e le libertà degli interessati;
- le minacce che potrebbero comportare accessi illegittimi;
- le modifiche indesiderate;
- l'indisponibilità dei dati.

F) ***documentazione delle decisioni assunte***

G) ***monitoraggio e revisione***

CONCLUDENDO: Il Regolamento Europeo prevede che l'inosservanza dei requisiti stabiliti per il DPIA può portare a sanzioni pecuniarie imposte dall'Ufficio del Garante. La mancata esecuzione di un DPIA nei casi in cui il trattamento è soggetto allo stesso, l'esecuzione in maniera errata del DPIA oppure la mancata consultazione dell'autorità di controllo laddove richiesta, possono comportare sanzioni amministrative pecuniarie elevatissime (addirittura fino a un importo massimo di 10 milioni di Euro)

A. *LA RETE INFORMATICA DELLA ISTITUZIONE SCOLASTICA*

La rete informatica è costituita da n° 8 stazioni di lavoro nel reparto amministrativo dotate di sistema operativo n.4 postazioni con Windows 7 Pro (da sostituire) n.4 con Windows 10 pro e dai seguenti server con SO Windows server 2019 essential.

L'abilitazione alla configurazione dei diritti di accesso è protetta da password in quanto sono inseriti in un Domain controller.

Il personale addetto è opportunamente istruito per gestire in modo autonomo il cambio della password di accesso al sistema e comunque coadiuvato da supporto tecnico.

Le stazioni di lavoro sono dotate di software antivirus Symentec Endpoint Server con aggiornamento automatico tramite internet e firewall installato di ultima generazione Microtik serie RB.

Inoltre l'Istituzione Scolastica si avvale del Responsabile esterno dei Dati gestito dalla Soc Axios che cura la seguente Banca Dati – gestionale operativo scuole

la rete è protetta da un sistema antivirus e antispyware che distribuisce gli aggiornamenti ai server e ai client sulla rete in automatico

B. (ANALISI DEI RISCHI, VULNERABILITÀ, PERICOLI)

In questa sezione vengono elencate e sviscerate le misure di sicurezza tecniche ed organizzative adottate o che si consigliano di adottare per la protezione dei dati personali trattati, rappresentando, altresì, che già l'Istituzione Scolastica, in ottemperanza alla circolare AGID 18 aprile 2017 n.2 - "*Misure minime di sicurezza ICT per le pubbliche amministrazioni*" e secondo quanto indicato nell'Allegato B del D.lgs. 196/03, ha adottato misure di sicurezza di natura informatica quali dettate dalla prefata circolare.

Alla luce di quanto previsto dagli artt. 35 e 36 del GDPR, la Istituzione Scolastica ha provveduto, altresì, ad avviare un processo finalizzato a descrivere il trattamento di dati personali, valutarne la necessità e la proporzionalità, nonché gestirne gli eventuali rischi per i diritti e le libertà delle persone fisiche da esso derivanti, effettuando una valutazione del livello del rischio e determinando le misure idonee a mitigarlo. Ciò secondo il nuovo approccio alla protezione dei dati personali voluto dal legislatore comunitario e fortemente basato sul principio della responsabilizzazione (*cd. accountability principle*).

Pertanto, propedeutica ad ogni azione si è effettuata l''analisi dei rischi che ha consentito di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi è consistita nella:

- individuazione di tutte le risorse del patrimonio informativo (dati obbligatori per disposizione di legge, relativi al personale dipendente in forza e cessato; elenco alunni; dati/informazioni di fornitori e clienti nei limiti necessari ad ottemperare alle disposizioni fiscali e contabili in vigore; documenti cartacei; hardware; software; apparecchiature di

comunicazione; servizi; immagine dell'Istituto);

- identificazione dei rischi cui tali risorse sono sottoposti;
- identificazione delle vulnerabilità;
- definizione delle contromisure;
- dati personali.

La classificazione dei **DATI PERSONALI** in funzione dell'analisi dei rischi è la seguente:

•***DATI ANONIMI,*** ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza se non quelle di tutela del patrimonio informativo dell'Istituto da perdite e/o danneggiamenti;

•***DATI PERSONALI***:

a) ***DATI PERSONALI COMUNI***
b) ***DATI PERSONALI PARTICOLARI ex art. 9 GDPR UE 679/2016***
c) ***DATI PERSONALI PARTICOLARI ex art. 10 GDPR UE GDPR UE 679/201***

2. INDIVIDUAZIONE DELLE RISORSE DA PROTEGGERE

E' emerso che le risorse da proteggere sono:

1. **LE BANCHE DATI;**
2. **ARCHIVIO PROTOCOLLO CON I DATI RELATIVI ALLA CORRISPONDENZA SPEDITA E RICEVUTA;**
3. **I DOCUMENTI CARTACEI;**
4. **L'HARDWARE;**
5. **IL SOFTWARE;**
6. **LE APPARECCHIATURE DI COMUNICAZIONE;**
7. **L'IMMAGINE DELL'ISTITUZIONE SCOLASTICA.**

2.1 Individuazione dei Pericoli

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse indicate sopra indicate.

Rischi	Deliberato	Accidental	Ambiental
Terremoto			**X**
Inondazione	**X**	**X**	**X**
Uragano			**X**
Fulmine			**X**
Danno volontario	**X**		
Interruzione di corrente	**X**	**X**	
Interruzione di acqua		**X**	
Interruzione di aria	**X**	**X**	
Guasto hardware		**X**	
Linea elettrica instabile		**X**	**X**
Temperatura e umidità			**X**
Polvere			**X**
Radiazioni		**X**	
Scariche elettrostatiche		**X**	
Furto	**X**		
Uso non autorizzato dei memoria	**X**		
Deterioramento dei supporti memoria		**X**	
Errore del personale		**X**	
Errore di manutenzione		**X**	
Masquerading dell'utente	**X**		
Uso illegale di software	**X**	**X**	
Software dannoso		**X**	
Esportazione/importazione software	**X**		
Accesso non autorizzato alla	**X**		
Uso della rete in modo non autorizzato	**X**		
Guasto tecnico di provider di		**X**	
Danni sulle linee	**X**	**X**	
Errore di trasmissione		**X**	

Sovraccarico di traffico	**X**	**X**
Intercettazione	**X**	
Infiltrazione nelle	**X**	
Analisi del traffico		**X**
Indirizzamento non corretto messaggi		**X**
Reindirizzamento dei	**X**	
Ripudio	**X**	
Guasto dei servizi di	**X**	**X**
Mancanza di personale		**X**
Errore dell'utente	**X**	**X**
Uso non corretto delle	**X**	**X**
Guasto software	**X**	**X**
Uso di software da parte di autorizzati	**X**	**X**
Uso di software in situazioni autorizzate	**X**	**X**

2.2 Individuazione delle Vulnerabilita'

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informatico che possono realizzarsi qualora si realizzasse uno dei pericoli indicati al punto 2.1

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte,finestre) **Mancanza di locali protetti per il server servere**	**Impiego di hw obsoleto quale sistema di** **rimpiazzo**	**Linee di comunicazione non protette**
Mancanza di controllo di accesso	**Suscettibilità a umidità, polvere, sporcizia**	**Giunzioni non protette**
Linea elettrica instabile - apparati di continuità obsoleti o fuori uso		**Mancanza di certificazione rete classe idonea**
		Mancanza di prova di ricezione/invio
		Presenza di linee dial-up (con modem)
		Mancanza strumenti di crittografia a protezione del traffico sensibile

Documenti cartacei	Software	Personale
Locali non protetti	**Errori noti del software**	**Carenza di personale**
Carente numero di distruggi- documenti per l'eliminazione	**Carenza di documentazione/formazione**	**Precaria supervisione degli esterni**
Assente controllo delle copie	**Incuria nella dismissione di di supporti riscrivibili**	**Formazione insufficiente sulla sicurezza**
	Permanenza di sessioni aperte senza utente	**Carente consapevolezza**
	Carenza di supporto o controllo nel caricamento del software	**Uso scorretto di hardware/software**

2.3 Individuazione dei Pericoli cui sono sottoposte le Risorse Hardware

I principali pericoli che possono incombere sulle risorse hardware sono:

1. malfunzionamenti dovuti a guasti;

2. malfunzionamenti dovuti a eventi naturali quali terremoti, allagamenti, incendi;

3. malfunzionamenti dovuti a blackout ripetuti ed in genere a sbalzi eccessivi delle linee di alimentazione elettrica;

4. malfunzionamenti dovuti a sabotaggi, furti, intercettazioni (apparati di comunicazione).

2.4 Individuazione dei Pericoli cui sono sottoposte le Risorse connesse in rete

I principali pericoli alle risorse connesse in rete possono provenire dall'interno del Teatro, dall'esterno o da una combinazione interno/esterno e sono relative:

1. all'utilizzo della LAN (pericoli interni);

2. ai punti di contatto con il mondo esterno attraverso Internet (pericoli esterni);

3. allo scaricamento di virus e/o trojan per mezzo di posta elettronica e/o alle operazioni di download eseguite tramite il browser (interni/esterni).

In riferimento a quest'ultimo punto si ritiene opportuno evidenziare le tecniche più in uso:

- ***IP SPOOFING***, l'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica;

- ***PACKET SNIFFING***, apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (hacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica, etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano /e informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso è possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker;

- ***PORT SCANNING***, serie programmata di tentativi di accesso diretti a evidenziare, in base alle "risposte" fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una "intrusione". Trattasi di un vero e proprio studio

delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo;

- ***HIGHJACKING***, intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l'hacker, simulando di essere un'altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L'operazione è complessa e richiede elevate capacità e rapidità d'azione;

- ***SOCIAL ENGINEERING,*** apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest'ultimo;

- ***BUFFER OVERFLOW***, azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di "amministratore del sistema", consentendo il controllo totale della macchina. L'hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;

- ***SPAMMING,*** saturazione di risorse informatiche a seguito dell'invio di un elevato numero di comunicazioni tali da determinare l'interruzione del servizio. Ad esempio l'invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi;

- ***PASSWORD CRACKING***, sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d'ordine;

- ***TROJAN,*** appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsciamente attivati dall'utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema;

- ***WORM,*** appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento);

- ***LOGIC BOMB***, appartengono alla categoria dei virus e sono programmi che contengono a/ proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall'attivazione;

- ***MALWARE E MMC (MALICIOUS MOBILE CODE***), costituiscono la

macrocategoria di codici avente come effetto il danneggiamento e l'alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses;

- ***DOS (DENIAL OF SERVICE***), attacco che mira a saturare le risorse di un servizio, di un server o di una rete;
- ***DDOS (DISTRIBUTED DENIAL OF SERVICE***), attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete.

2.5 Individuazione dei Pericoli cui sono sottoposti i Dati trattati

I principali pericoli sui dati trattati sono:

1. accesso non autorizzato agli archivi contenenti le informazioni riservate da parte di utenti interni e/o esterni;
2. modifiche accidentali agli archivi da parte di utenti autorizzati.

2.6 Individuazione dei Pericoli cui sono sottoposti i Supporti di memorizzazione

I principali pericoli sui supporti di memorizzazione sono:

- distruzione e/o alterazione a causa di eventi naturali;
- imperizia degli utilizzatori;
- sabotaggio;
- deterioramento nel tempo (invecchiamento dei supporti);
- difetti di costruzione del supporto di memorizzazione che ne riducono la vita media;
- evoluzione tecnologica del mercato che rende in breve tempo obsoleti alcuni tipi di supporti.

3. INDIVIDUAZIONE DELLE CONTROMISURE

In questa parte del documento vengono descritte le misure adottate e da adottare per annullare o limitare le **Vulnerabilità** e contrastare i **Pericoli**. Per **misura** viene intesa lo specifico intervento di carattere fisico, procedurale,elettronico/informatico posto in essere o da per in essere per prevenire, contrastare o ridurre gli effetti relativi

ad una specifica minaccia, nonché per assicurare il livello minimo di protezione.

3.1 Contromisure di carattere fisico e procedurale

Contro i rischi di intrusione i locali sono dotati di impianto di allarme, attivabile dal personale dipendente.

L'attivazione di detto sistema di allarme avviene al termine dell'orario di lavoro. Le aree contenenti dati in supporto cartaceo (mobili ed armadi contenenti documenti) sono ubicate in modo tale che ciascun addetto possa rilevare a vista il tentativo di accesso da parte di persone estranee e, di conseguenza, impedirne l'accesso stesso. L'ubicazione di stampanti non consente ad estranei di leggere od asportare eventualmente documenti non ancora prelevati dal personale. Il personale amministrativo, incaricato del trattamento, ha ricevuto le opportune istruzioni per la tutela e la protezione dei dati in formato cartaceo e dei dispositivi informatici attraverso i quali avviene il trattamento dei dati personali.

L'accesso ai locali in cui avviene il trattamento e la custodia di dati personali è vigilato dai Collaboratori Scolastici cui è assegnato il compito di impedire l'intrusione da parte di persone non autorizzate e di identificare e quindi verificare l'autorizzazione all'accesso ai locali dei soggetti ammessi dopo l'orario di chiusura degli uffici.

In riferimento ai supporti cartacei, sono state impartite dettagliate istruzioni per la protezione dei quali

- qualsiasi documento presentato alla scuola va inserito, quando personale, in apposite cartelline non trasparenti;
- qualsiasi documento che l'istituzione scolastica consegni agli utenti va inserito, quando riservato o contenente documentazione sensibile, in apposite buste o cartelline non trasparenti;
- eventuali rubriche telefoniche in utilizzo su supporto cartaceo debbono essere richiuse dopo la consultazione ed il primo foglio delle rubriche stesse, leggibile dall'esterno, non deve contenere alcun dato (praticamente il primo foglio funge da copertina);
- è permesso l'accesso ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;

- è fatto divieto di fotocopiare/scannerizzare documenti senza l'autorizzazione del Responsabile interno del trattamento;
- massima attenzione dovrà essere posta ai documenti che si trovano in locali accessibili al pubblico;
- è fatto divieto di esportare documenti o copie dei medesimi all'esterno. Tutti i documenti cartacei devono essere gestiti in modo da ridurre al minimo i tempi di permanenza al di fuori degli archivi o degli armadi o dei contenitori in dotazione alle unità operative;
- l'accesso agli archivi è consentito al personale a ciò espressamente autorizzato in via permanente od occasionale;
- E' fatto divieto di fotocopiare, passare allo scanner e comunque riprodurre documenti senza l'autorizzazione del Responsabile interno del trattamento;
- gli archivi devono essere mantenuti costantemente chiusi, compatibilmente con le esigenze di servizio. Le copie dei documenti e/o scansioni vanno trattate, con riferimento alla tutela dei dati personali in esse contenuti, con la medesima diligenza riservata agli originali;
- gli Incaricati che possono essere trattati Dati Particolari, hanno ricevuto dettagliate istruzioni onde porre massima attenzione al rispetto delle disposizioni precedenti. Essi, inoltre, dovranno limitare al minimo indispensabile la giacenza della documentazione al di fuori degli armadi o contenitori muniti di serratura; controllare con particolare rigore l'accesso ai propri archivi, autorizzare e registrare eventuali accessi negli uffici compiuti al di fuori degli usuali orari di lavoro;
- Gli Incaricati nominati sono responsabili della riservatezza dei registri in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio, e comunque quando non necessario all'espletamento dei compiti, i registri devono essere conservati negli appositi armadi/cassetti chiusi a chiave; una chiave di riserva è mantenuta con le dovute cautele dal Responsabile del trattamento in armadietto chiuso a chiave;
- il protocollo riservato, accessibile solo al Titolare e al Responsabile interno del trattamento è conservato nell' ufficio del Dirigente Scolastico;

- la responsabilità del controllo sui documenti stampati è del Responsabile del trattamento. Il materiale cartaceo destinato allo smaltimento dei rifiuti deve essere ridotto in frammenti: all'uopo vi è in dotazione apposito macchinario distruggi documenti
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento.

3.2 Contromisure di carattere elettronico/informatico

In riferimento alle misure di carattere elettronico/informatico sono state impartite dettagliate istruzioni per la protezione quali:

- Utilizzo di server con configurazioni di ridondanza;
- presenza di gruppi di continuità elettrica per il server;
- attivazione di un sistema di backup automatizzato con periodicità settimanale e una copia storica ad un mese. Le copie di backup realizzate giornalmente debbono essere conservate in un armadio di ferro chiuso a chiave possibilmente ignifugo;
- firewall ridondante che protegge la rete dagli accessi indesiderati attraverso internet;
- la navigazione degli utenti è filtrata ed è bloccata la consultazione dei siti i cui URL appartengono alle sotto elencate categorie:

Adult/Sexually Explicit	Siti per adulti/Sesso esplicito
Chat	Chat
Criminal Skills	Siti riguardanti lo criminalità
Drugs, Alcohol & Tabacco	Droga, Alcool e Tabacco
Food Drink	Siti riguardanti la ristorazione

Gambling	Scommesse
Games	Giochi
Glamour & Intimate Apparel	Biancheria ed Intimo
Hacking	Pirateria informatica
Hate Speech	Incitamento all'odio
Hobbies & Recreation	Hobbies e divertimento
Kid's Sites	Siti con contenuti su minori
Motor Vehicles	Siti riguardanti i motori
Personals & Dating	Chat con informazioni personali
Religion	Siti riguardanti argomenti religiosi
Sex Education	Educazione sessuale
Sports	Sports
Violence	Siti riguardanti argomenti di violenza
Weapons	Armi

3.3 Regole di gestione e regole di comportamento

- ***DEFINIZIONE DELLE REGOLE PER LA GESTIONE DI PASSWORD SUI SISTEMI OPERATIVI***

    a. l'accesso al sistema informativo degli incaricati del trattamento dei dati personali è permesso per mezzo di un codice identificativo personale (user-id) e password personale;

    b. al primo accesso, la password ottenuta dal Custode delle password deve essere cambiata;

    c. la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;

    d. deve successivamente essere cambiata almeno ogni sei mesi;

    a. è segreta e non deve essere comunicata ad altri;

b. va custodita con diligenza e riservatezza;

c. l'utente deve sostituire la password, nel caso ne accertasse la perdita; le password verranno automaticamente disattivate dopo tre mesi di non utilizzo a cura del Servizio Informatico;

d. in caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dal custode delle password al tecnico/sistemista addetto alla manutenzione le credenziali di **autenticazione di servizio**. Al termine delle operazioni di manutenzione il custode deve ripristinare **nuove credenziali** di autenticazione

- ***INDICAZIONE DELLE REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS***:

a. limitare lo scambio fra computer di supporti rimovibili (floppy, cd, pen drive, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC, XLS;

b. controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;

c. evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal Responsabile del Servizio Informatico;

d. disattivare gli Activex e il download dei file per gli utenti del browser Internet Explorer;

e. disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);

f. attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate, possono infettare il computer);

g. non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza

anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e dalla rubrica di un computer infettato per inviare nuovi messaggi "infetti");

h. non cliccare mai su di un link presente in un messaggio di posta elettronica da provenienza sconosciuta, (in quanto potrebbe essere falso e portare a un sito-truffa);
i. non utilizzare le chat;
j. seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);

- ***INDICAZIONE DELLE REGOLE DI COMPORTAMENTO IN CASO DI SISTEMI DANNEGGIATI DA VIRUS.***

Il Titolare del trattamento, attraverso l'Amministratore di Sistema o dei tecnici incaricati per gli interventi sul sistema informatico. procede a reinstallare il sistema operativo, i programmi applicativi e i dati seguendo la procedura indicata:

a. formattare l'Hard Disk, definire le partizioni e reinstallate il Sistema Operativo;
b. installare il software antivirus, verificare e installare immediatamente gli eventuali ultimi aggiornamenti;
c. reinstallare i programmi applicativi a partire dai supporti originali;
d. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
e. effettuare il RESTORE dei soli dati a partire da una recente copia di BACKUP;
f. ***NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP,*** in quanto potrebbe essere infetta;
g. ricordare all'utente di prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine;

3.4 Incident Response e Ripristino

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il Responsabile interno del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

1. discrepanze nell'uso degli user-id;
2. modifica e sparizione di dati;
3. cattive prestazioni del sistema (così come percepite dagli utenti);

4. irregolarità nell'andamento del traffico;
5. irregolarità nei tempi di utilizzo del sistema;
6. quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine della Istituzione Scolastica;
5. garantita l'incolumità fisica alle persone procedendo ad isolare l'area contenente il sistema oggetto dell'incidente; isolare il sistema compromesso dalla rete e successivamente spegnere correttamente il sistema.

Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso.

3.5 Il Penetration Test

- ***Il Pen Test*** è una tipologia di analisi di un sistema informatico indispensabile per valutare la sicurezza di un sistema informatico, in quanto permette la individuazione di eventuali punti deboli, difetti tecnici e vulnerabilità. Queste problematiche possono derivare dalla progettazione, implementazione o gestione del sistema, e potrebbero essere sfruttate per compromettere gli obiettivi di sicurezza del sistema. A tal fine sarà compito dell'Amministratore di Sistema alias ***Chief Information Security Officier*** - in stretto collegamento con il **Data Protection Officer -** attivarsi per:

- valutare le vulnerabilità che possono interessare la rete, gli apparati, le applicazioni e i servizi proponendo soluzioni ed accorgimenti pratici, nonché realizzare nuovi prodotti e servizi di security.

- monitorare i sistemi e proporre soluzioni relative alla risposta agli incidenti nonché ricercare costantemente soluzioni volte a migliorare la sicurezza dell'organizzazione.

- svolgere l'assessment delle soluzioni di security presenti nella scuola e di curare il disegno armonico e coerente delle misure di sicurezza.

- sviluppare e monitorare sistemi di risposta , in tempo reale, in grado di identificare e trattare possibili minacce in modo automatico e cognitivo.

- rendere operative le soluzioni tecnologiche di security, dalla introduzione alla manutenzione e al supporto agli utenti finali.

- occuparsi dello sviluppo di specifiche soluzioni di security così come dell'integrazione di servizi svolti da terzi.

con la conoscenza delle principali modalità di attuazione di penetration test, simulare operazioni in grado di dimostrare l'effettiva pericolosità di alcune vulnerabilità di cui soffre la scuola, nonché i fattori di debolezza nella strategia di security dell'organizzazione

3.5 Piano di formazione

La formazione degli sub responsabili/incaricati viene effettuata all'ingresso in servizio e all'installazione di nuovi strumenti per il trattamento dei dati. Inoltre è prevista la formazione specifica ex GDPA 679/2016.
Le finalità della formazione sono:

1. sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
2. proporre buone pratiche di utilizzo sicuro della rete;
3. riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

Il piano prevede inoltre la pubblicazione di normativa ed ordini di servizio.

4. Norme per il Personale

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse informatiche loro assegnate per lo svolgimento dell'attività lavorativa , nel rispetto di quanto stabilito nel presente Documento, dalle prescrizioni dettate nelle lettere d'incarico e dall'allegato "Regolamento per l'uso della Rete Informatica"..

5. Smaltimento Rifiuti Apparecchiature Elettroniche e Misure di Sicurezza dei Dati Personali

Lo smaltimento corretto dei prodotti tecnologici è una questione che sta investendo in maniera sempre più evidente la corretta gestione delle informazioni. Si ponga mente, ad esempio, al ricambio necessitato e sempre più rapido degli strumenti informatici da cui l rischi incontrollati di perdita e dispersione di dati:. rischi che possono produrre eventi molto dannosi quali il furto di identità. Già nel 2008, il Garante Privacy aveva chiarito che ogni titolare del trattamento, in considerazione del rischio elevato di circolazione di componenti elettroniche contenenti dati personali che non siano stati cancellati in modo idoneo, "*è tenuto ad adottare appropriate misure organizzative e tecniche volte a garantire la sicurezza dei dati personali trattati, nonché*

la loro protezione nei confronti di accessi non autorizzati, che possono verificarsi in occasione della dismissione dei menzionati apparati elettrici ed elettronici".

Il Garante Privacy aveva suggerito alcuni accorgimenti che consistevano:
1) in misure tecniche preventive per la memorizzazione sicura dei dati, applicabili a dispositivi elettronici o informatici (per esempio: l'utilizzo della cifratura dei dati;
2) in misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici (per esempio: formattazione "a basso livello" dei dispositivi di tipo hard disk o quando possibile demagnetizzazione dei dispositivi di memoria);
3) in misure specifiche per lo smaltimento di rifiuti elettrici ed elettronici (per esempio: la distruzione dei supporti di memorizzazione di tipo ottico o magneto-ottico).Si ritiene che questi suggerimenti siano ancora validi.

6. Aggiornamento del Data Protection Impact Assessment

Il ***DPIA*** è soggetto a revisione almeno annua.
Comunque deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo dell'Istituto ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo dell'Istituto Scolastico tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

PARTE TERZA

CONCLUSIONI DERIVANTI DALL'ANALISI DEI RISCHI

L'analisi dei rischi collegati alle vulnerabilità del sistema informatico e conseguentemente ai pericoli del realizzarsi di "*eventi negativi*" che potrebbero verificarsi in danno dei dati personali trattati, ha tenuto presente la seguente ***MATRICE DEL RISCHIO*** che si fonda sulle conosciute categorie di ***probabilità*** che l'evento dannoso si realizzi e ***gravità*** degli eventuali danni in caso di realizzazione dell'effetto dannoso. Le categorie di probabilità e gravita sono ben note in materia di calcolo del rischio ex T.U. 81/2008 s.m.i.

Scala della probabilità					
	Molto probabile	4	5	6	7
	Probabile	3	4	5	6
	Poco probabile	2	3	4	5
	Improbabile	1	2	3	4
		Bassa	Media	Alta	Altissima
	Scala della Gravità				

Per le contromisure in atto o previste si ritiene potere affermare che il **rischio per il trattamento dei dati cartacei** può essere considerato ***BASSO***

Analogamente il **rischio per il trattamento dei dati elettronici** può essere considerato ***BASSO*** in quanto **i rischi relativi agli strumenti elettronici,** dalla analisi effettuata possono ritenersi ***BASSI*** così come **i rischi relativi ai software**

PARTE QUARTA

GLI ALLEGATI

ALLEGATO n° 1 GLOSSARIO

- ***Titolare del trattamento***: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) che, singolarmente o insieme ad altri (contitolare del trattamento), determina le finalità e i mezzi del trattamento di dati personali
- ***Rappresentante del Titolare del trattamento***: la persona fisica o giuridica stabilita nel territorio dell'Unione europea, designata dal Titolare non stabilito nell'Unione affinché lo rappresenti per quanto riguarda gli obblighi previsti dal Regolamento
- ***Responsabile della protezione dei dati (DPO)***: il soggetto, interno o esterno alla struttura del Titolare, che in piena indipendenza e autonomia supporta quest'ultimo in merito all'applicazione degli obblighi previsti dal Regolamento, organizza e sorveglia la gestione dei trattamenti e funge da punto di contatto per le questioni in tema di privacy. La figura è obbligatoria quando le attività principali del Titolare consistono in trattamenti che richiedono il monitoraggio regolare e sistematico degli interessati su larga scala oppure in trattamenti su larga scala di dati particolari (ex sensibili) e "giudiziari"

- ***Responsabile del trattamento***: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) esterno alla struttura del Titolare del trattamento che tratta dati personali per conto di quest'ultimo
- ***Sub-responsabile del trattamento***: il soggetto (la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) cui il Responsabile del trattamento ricorre per l'esecuzione di specifiche attività di trattamento di dati personali per conto di quest'ultimo. Il ricorso al Sub-responsabile deve essere preventivamente autorizzato per iscritto dal Titolare.
- ***Delegato dal Titolare del trattamento — Referente privacy***: figura facoltativa, a cui il Titolare può ricorrere a fini meramente organizzativi e che potrebbe sostituire il vecchio "responsabile interno"
- ***Ufficio di riferimento:*** ufficio o funzione che cura prioritariamente il trattamento
- ***Interessato***: la persona fisica identificata o identificabile cui si riferiscono i dati
- ***Categorie di interessati:*** es. dipendenti, alunni, familiari degli alunni, soggetti terzi (altri utenti,fornitori, professionisti, ecc.),altre Pubbliche Amministrazioni
- ***Dato personale***: qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. Si distingue:
    - **Dati comuni**: es. anagrafici (nome, cognome, data di nascita, cittadinanza, stato civile, indirizzo, qualifica professione); documenti di identità (Cdl, patente, passaporto); codici di identificazione fiscale (CF, partita IVA persone fisiche); dati di contatto (numero di telefono, indirizzo e-mail, indirizzo fisico); codici identificativi lavoratori (matricola, credenziali di accesso ai sistemi informatici); coordinate bancarie (numero CC, codice IBAN); targa veicolo; dati multimediali (vide, audio); dati di navigazione internet (cookie, log, indirizzo IP); dati di geolocalizzazione; dati di profilazione.
    - **Dati particolari previsti dall'art. 9 Regolamento Europeo 679/2018**: es. dati idonei a rivelare l'appartenenza a partiti, sindacati, organizzazioni a carattere religioso o filosofico; dati genetici; dati biometrici; dati relativi alla salute (es. gravidanza, malattia, appartenenza a categorie protette)
    - **Dati previsti dall'art.10 Regolamento Europeo 679/2018:** es. dati relativi a condanne penali, ai reati e alle connesse misure di sicurezza (es. dati in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti).

- **Informazioni non considerate dati personali**: es. informazioni riconducibili a un soggetto non persona fisica; numero di iscrizione al registro delle imprese di una società; indirizzo e-mail, come info@azienda.com; dati resi anonimi.

- ***Destinatario***: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Es. Responsabile del trattamento (anche semplicemente per categoria di appartenenza), persone autorizzate al trattamento (incaricati del trattamento), imprese del gruppo, associazioni di imprese, sindacati, imprese assicurative
- ***Legittimo interesse del titolare o di un terzo***: basi giuridiche del trattamento a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato e tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare. Affinché il legittimo interesse possa operare come base giuridica del trattamento è necessario, tra l'altro, che:
  b) il trattamento non abbia a oggetto dati "particolari" compresi quelli biometrici o "giudiziari";
  c) non operi un'ulteriore base giuridica (es. adempimento di un obbligo legale oppure l'esecuzione di un contratto del quale è parte l'interessato o di misure precontrattuali);
  d) le finalità perseguite sia individuate specificamente, in modo da predisporre garanzie adeguate (es. in ambito lavorativo, il legittimo interesse del datore di lavoro può essere invocato come presupposto di liceità a condizione che il trattamento dei dati dei lavoratori sia strettamente necessario per uno scopo legittimo e conforme ai principi di proporzionalità e sussidiarietà);
  e) prima di procedere al trattamento, sia effettuata la valutazione di impatto qualora sia effettuato con nuove tecnologie o strumenti automatizzati.

ALLEGATO n° 2 LA NORMATIVA

Articolo 30 GDPR UE 679/2016 : Registri delle attività di trattamento

Ogni titolare del trattamento e, ove applicabile, il suo rappresentante tengono un registro delle attività di trattamento svolte sotto la propria responsabilità. Tale registro contiene tutte le seguenti informazioni:

a) *il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;*

b) *le finalità del trattamento;*

c) *una descrizione delle categorie di interessati e delle categorie di dati personali;*

d) *le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;*

e) *ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*

f) *ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;*

g) *ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.*

Ogni responsabile del trattamento e, ove applicabile, il suo rappresentante tengono un registro di tutte le categorie di attività relative al trattamento svolte per conto di un titolare del trattamento, contenente:

- *il nome e i dati di contatto del responsabile o dei responsabili del trattamento, di ogni titolare del trattamento per conto del quale agisce il responsabile del trattamento, del rappresentante del titolare del trattamento o del responsabile del trattamento e, ove applicabile, del responsabile della protezione dei dati;*
- *le categorie dei trattamenti effettuati per conto di ogni titolare del trattamento;*
- *ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;*
- *ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.*

  I registri di cui ai paragrafi 1 e 2 sono tenuti in forma scritta, anche in formato elettronico o Su richiesta, il titolare del trattamento o il responsabile del trattamento e, ove applicabile, il rappresentante del titolare del trattamento o del responsabile del trattamento mettono il registro a disposizione dell'autorità di controllo.

  Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, il trattamento non sia occasionale o includa il trattamento di categorie particolari

di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10."

ALLEGATO n° 3

REGOLAMENTO DELLA ISTITUZIONE SCOLASTICA PER L'UTILIZZO DEL SISTEMA INFORMATICO, DEI TELEFONI " FISSI", DEI "CELLULARI" E DEI " TABLET "

INDICE

Art. 12 I Controlli
Art. 13 Obbligatorietà e Sanzioni
Art. 14 Gestione della casella di Posta Elettronica del Lavoratore cessato dal servizio
Art. 15 Esercizio dei diritti
Art. 16 Aggiornamento e Revisione

Premesse

In via preliminare devesi precisare che il presente Regolamento si applica a:

- tutti i Lavoratori, a qualsiasi titolo inseriti nell'organizzazione scolastica, senza distinzione di ruolo e/o mansione;
- a tutti i collaboratori dell'Amministrazione, a prescindere dal rapporto contrattuale intrattenuto con la stessa

Tanto precisato deve dirsi che l'utilizzo delle risorse informatiche e telematiche della Istituzione Scolastica Istituto Comprensivo Piazza Filattiera 84 deve sempre ispirarsi al principio della diligenza e correttezza, comportamenti che normalmente si adottano nell'ambito di un rapporto di lavoro. Pertanto la Istituzione Scolastica ha adottato un Regolamento interno diretto ad evitare che comportamenti inconsapevoli possano innescare problemi o minacce alla Sicurezza nel trattamento dei dati. E' evidente, infatti che la progressiva diffusione delle nuove tecnologie informatiche, ed in particolare il libero accesso alla rete Internet dai Personal Computer, espone la Istituzione Scolastica ai rischi di un coinvolgimento in tema di responsabilità civili ,penali ed amministrative, creando problemi alla sicurezza e all'immagine della Istituzione Scolastica stessa. Per l'Amministrazione l'utilizzo improprio, da parte del Lavoratore, di Posta Elettronica, Internet e telefoni fissi, può pregiudicare il regolare funzionamento delle installazioni tecniche o altri beni o interessi meritevoli di tutela e/o giuridicamente protetti, fra cui:

a) economie dei costi;
b) la capacità di memoria utilizzabile dei server o l'ampiezza di banda disponibile per il collegamento in rete;
c) sicurezza delle applicazioni e dei dati (disponibilità, integrità, confidenzialità);
d) produttività sul lavoro;
e) la reputazione o l'immagine della Istituzione Scolastica;

f) responsabilità oggettiva della Istituzione Scolastica, ex art. 2049 CC, per comportamenti illeciti dei propri dipendenti.

Per il Lavoratore, i rischi derivanti dall'utilizzo di Posta Elettronica, Internet e telefoni , riguardano:

1. la protezione dei dati personali, propri e di terzi, poiché i predetti strumenti lasciano "tracce" del loro uso;
2. la possibilità che l'Istituzione Scolastica, in fase di eventuale legittimo controllo, venga a conoscenza di dati od opinioni personali del Lavoratore;
3. relativamente all'uso di Posta Elettronica e di Internet, l'introduzione di virus, worm, cavalli di Troia o installazioni di programmi estranei nel computer utilizzato dal Lavoratore, con conseguente perdita di tutti o parte dei file salvati sul medesimo computer.

Si ritiene opportuno dettare ,altresì, norme sull'utilizzo della posta elettronica della istituzione scolastica dei telefoni fissi,mobili e tablet.

A tal fine con il presente Regolamento si disciplinano le modalità di utilizzo:

- **del PERSONAL COMPUTER;**
- **della RETE INTERNET E RELATIVA GESTIONE DELLE PASSWORD**
- **dei SUPPORTI MAGNETICI RIUTILIZZABILI (DISCHETTI,CARTUCCE, ECC…..);**
- **dei PC PORTATILI;**
- **della POSTA ELETTRONICA DELLA ISTITUZIONE SCOLASTICA dei TELEFONI FISSI,MOBILI E TABLET**

Art.1 Utenti autorizzati all'uso di Internet

Per quanto riguarda l'uso delle dotazioni informatiche e l'accesso ad internet si individuano 4 tipologie di utenti:

- **Personale tecnico**: autorizzato all'uso limitatamente allo svolgimento delle proprie mansioni o alle disposizioni ricevute
- **Personale amministrativo**: autorizzato all'uso per lo svolgimento dell'attività amministrativa
- **Personale docente:** autorizzato all'uso per qualunque attività educativa, didattica e formativa o ad esse anche indirettamente collegata.
- **Alunni**: autorizzati limitatamente all'attività educativa, didattica e formativa programmata dai docenti

Art.2 Utilizzo del Personal Computer

Il Personal Computer affidato al dipendente è uno **strumento di lavoro** per cui ogni utilizzo non inerente all'attività lavorativa può contribuire ad innescare disservizi, costi di manutenzione e, soprattutto, minacce alla sicurezza.

L'accesso all'elaboratore è protetto da password che deve essere custodita dall'incaricato con la massima diligenza e non divulgata. La stessa password deve essere attivata per l'accesso alla rete, per lo screen saver e per il collegamento a Internet. Non è consentita l'attivazione della password di accensione (bios), senza preventiva autorizzazione da parte del Titolare o del Responsabile interno del trattamento dei dati

Il custode delle parole chiave riservate**,** per l'espletamento delle sue funzioni, ha la facoltà in qualunque momento di accedere ai dati trattati da ciascuno, ivi compresi gli archivi di posta elettronica interna ed esterna.

Il custode delle parole chiave riservate potrà accedere ai dati ed agli strumenti informatici esclusivamente per permettere alla stessa azienda, titolare del trattamento, di accedere ai dati trattati da ogni incaricato con le modalità fissate dalla stessa azienda, al solo fine di garantire l'operatività, la sicurezza del sistema ed il normale svolgimento dell'attività aziendale nei casi in cui si renda indispensabile ed indifferibile l'intervento, ad esempio in caso di prolungata assenza od impedimento dell'incaricato, informando tempestivamente l'incaricato dell'intervento di accesso realizzato.

Non è consentito installare autonomamente programmi provenienti dall'esterno salvo previa autorizzazione esplicita del Titolare o del Responsabile interno del trattamento dei dati in quanto sussiste il grave pericolo di portare Virus informatici e di alterare la stabilità delle applicazioni dell'elaboratore.

Non è consentito l'uso di programmi diversi da quelli distribuiti ed installati ufficialmente su richiesta del Titolare o del Responsabile interno del trattamento dei dati. L'inosservanza di questa disposizione, infatti, oltre al rischio di danneggiamenti del sistema per incompatibilità con il software esistente, può esporre l'azienda a gravi responsabilità amministrative, civili ed anche penali in caso di violazione della normativa a tutela dei diritti d'autore sul software (D. Lgs. 518/92 s.m.i. sulla tutela giuridica del software e L. 248/2000 s.m.i. nuove norme di tutela del diritto d'autore) che impone la presenza nel sistema di software regolarmente licenziato o comunque libero e quindi non protetto dal diritto d'autore.

Non è consentito all'utente modificare le caratteristiche impostate sul proprio PC, salvo previa autorizzazione esplicita del Titolare o del Responsabile interno del trattamento dei dati.

Il Personal Computer deve essere spento ogni sera prima di lasciare gli uffici o in caso di assenze prolungate dall'ufficio. In ogni caso lasciare un elaboratore incustodito connesso alla rete può essere causa di utilizzo da parte di terzi senza che vi sia la possibilità di provarne in seguito l'indebito uso. In ogni caso deve essere attivato lo screen saver e la relativa password.

Non è consentita l'installazione sul proprio PC di nessun dispositivo di memorizzazione, comunicazione o altro (come ad esempio masterizzatori, modem, …), se non con l'autorizzazione espressa del Titolare o del Responsabile interno del trattamento dei dati.

Ogni utente deve prestare la massima attenzione ai supporti di origine esterna, avvertendo immediatamente il Responsabile interno del trattamento dei dati nel caso in cui vengano rilevati virus.

Art.3 Utilizzo della Rete

Le unità di rete sono aree di condivisione di informazioni strettamente professionali e non possono in alcun modo essere utilizzate per scopi diversi. Pertanto qualunque file che non sia legato all'attività lavorativa non può essere dislocato, nemmeno per brevi periodi, in queste unità. Su queste unità, vengono svolte regolari attività di controllo, amministrazione e backup.

Le password d'ingresso alla rete ed ai programmi sono segrete e vanno comunicate e gestite secondo le procedure impartite. È assolutamente proibito entrare nella rete e nei programmi con altri nomi utente.

il Responsabile interno del trattamento dei dati può in qualunque momento dare disposizioni di procedere alla rimozione di ogni file o applicazione che riterrà essere pericolosi per la Sicurezza sia sui PC degli incaricati sia sulle unità di rete.

Costituisce buona regola la periodica (almeno ogni sei mesi) pulizia degli archivi, con cancellazione dei file obsoleti o inutili. Particolare attenzione deve essere prestata alla duplicazione dei dati. È infatti assolutamente da evitare un'archiviazione ridondante.

L' utente deve effettuare la stampa dei dati solo se strettamente necessaria e di ritirarla prontamente dai vassoi delle stampanti comuni. È buona regola evitare di stampare documenti o file non adatti (molto lunghi o non supportati, come ad esempio il formato pdf o file di contenuto grafico) su stampanti comuni. In caso di necessità necessità la stampa in corso può essere cancellata.

Art.4 Uso della Rete Internet e dei relativi servizi

Il PC abilitato alla navigazione in Internet costituisce uno strumento necessario allo svolgimento della propria attività lavorativa: pertanto è assolutamente proibita la navigazione in Internet per motivi diversi da quelli strettamente legati all'attività lavorativa stessa.

È fatto divieto all'utente lo scarico di software gratuito (freeware) e shareware prelevato da siti Internet, se non espressamente autorizzato dal responsabile interno del trattamento dei dati.

È tassativamente vietata l'effettuazione di ogni genere di transazione finanziaria ivi comprese le operazioni di remote banking, acquisti on-line e simili salvo i casi direttamente autorizzati dal Titolare o dal responsabile interno del trattamento dei dati personali e con il rispetto delle normali procedure di acquisto.

È da evitare ogni forma di registrazione a siti i cui contenuti non siano legati all'attività lavorativa.

È vietata la partecipazione a Forum non professionali, l'utilizzo di chat line (esclusi gli strumenti autorizzati), di bacheche elettroniche e le registrazioni in guest books anche utilizzando pseudonimi (o nicknames).

Art.5 Gestione delle Password

Le password di ingresso alla rete, di accesso ai programmi e dello screen saver, sono previste ed attribuite dal custode delle password, su disposizione del Responsabile Interno del Trattamento dei dati È necessario procedere alla modifica della password a cura dell'incaricato del trattamento al primo utilizzo e, successivamente, almeno ogni sei mesi; nel caso di trattamento di dati sensibili e di dati giudiziari la periodicità della variazione deve essere ridotta a tre mesi con contestuale comunicazione al Custode delle chiavi.

Le password possono essere formate da lettere (maiuscole o minuscole) e numeri ricordando che lettere maiuscole e minuscole hanno significati diversi per il sistema; **;** devono essere composte da almeno otto caratteri e non deve contenere riferimenti agevolmente riconducibili all'incaricato .

La password deve essere immediatamente sostituita, dandone comunicazione al Custode delle chiavi, nel caso si sospetti che la stessa abbia perso la segretezza.

Qualora l'utente venisse a conoscenza delle password di altro utente, è tenuto a darne immediata notizia al Responsabile interno del trattamento dei dati.

Art.6 Utilizzo di PC portatili

L'utente è responsabile del PC portatile assegnatogli dal Responsabile del Trattamento dei Dati e deve custodirlo con diligenza sia durante gli spostamenti sia durante l'utilizzo sul luogo di lavoro.

Ai PC portatili si applicano le regole di utilizzo previste per i PC connessi in rete, con particolare attenzione alla rimozione di eventuali file elaborati sullo stesso prima della riconsegna.

I PC portatili utilizzati all'esterno (convegni, stage, viaggi d'istruzione , ecc…), in caso di allontanamento, devono essere custoditi in un luogo protetto.

Art.7 Utilizzo dei Supporti Magnetici

Tutti i supporti magnetici riutilizzabili contenenti dati particolari previsti dagli artt. 9 e 10 GDPR 679/2016 devono essere trattati con particolare cautela onde evitare che il loro contenuto possa essere recuperato. Terzi particolarmente esperti, infatti, potrebbero recuperare e impossessarsi dei dati memorizzati anche dopo la loro cancellazione.

I supporti magnetici contenenti i prefati dati particolari devono essere custoditi in archivi chiusi a chiave.

Art. 8 Uso dei telefoni "fissi" sul posto di lavoro

1. I telefoni "fissi" che l'Amministrazione mette a disposizione devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.
2. Solo in caso di particolare necessità e/o urgenza, i Lavoratori possono utilizzare tali beni per motivi non attinenti l'attività lavorativa e, comunque, non in modo ripetuto o per periodi di tempo prolungati. E' comunque preferibile, laddove possibile, che i Lavoratori utilizzino i propri telefoni cellulari.
   Al fine di consentire il monitoraggio dei costi delle linee telefoniche, verrà fornito al Titolare del trattamento l'elenco delle telefonate effettuate dagli apparecchi di propria competenza completo di numeri telefonici chiamati (con le ultime tre cifre oscurate) e del relativo costo.
3. L'Amministrazione raccoglie i log files per redigere analisi statistiche dirette al perseguimento di finalità organizzative, produttive e di sicurezza.
   I dati raccolti, che sono trattati nel rispetto delle leggi di volta in volta in vigore, vengono conservati per il tempo strettamente necessario alle suddette analisi e finalità. In caso di anomalie riscontrate nelle modalità di utilizzo del telefono aziendale, si applicherà quanto previsto dall' art. 13 del presente disciplinare.

Art. 9 Uso dei telefoni "cellulari" e dei "palmari"

1. I telefoni "cellulari" e " tablet " che l'Amministrazione può mettere a disposizione, su richiesta motivata del Dipendente,devono essere utilizzati in modo strettamente pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale.
2. Il Lavoratore assegnatario di un telefono "cellulare", di un " tablet dell'Amministrazione è responsabile del suo utilizzo e della sua custodia.
3. All'utilizzo del telefono "cellulare", o del "palmare" dell'Amministrazione si applicano le medesime regole previste

Art.10 Intranet e dominio istruzione.it

I servizi di posta elettronica del dominio ***istruzione.it,*** quelli forniti dal sito ***www.istruzione.it*** e dalla intranet ministeriale sono direttamente gestiti dalla **Direzione Generale per i Sistemi Informativi** che ha diffuso specifiche informative in merito alle modalità di utilizzo dei suddetti servizi.

Art. 11 Utilizzo del servizio di Posta Elettronica della Istituzione Scolastica

- La Posta Elettronica che l'Istituzione Scolastica mette a disposizione deve essere utilizzata in modo pertinente allo svolgimento dell'attività lavorativa, secondo un utilizzo appropriato, efficiente, corretto e razionale nel rispetto del principio di riservatezza. I Lavoratori assegnatari delle caselle di Posta Elettronica sono

responsabili del corretto utilizzo delle stesse e vi accedono mediante autenticazione informatica user-id e password oppure altro sistema identificativo ad es. smart card.

- I Lavoratori sono tenuti, in un'ottica di correttezza ed uso responsabile degli strumenti, a contribuire alla riduzione del fenomeno dello "spam" (trasmissione su larga scala e in grandi volumi di e-mail non sollecitati): evitando di rispondere e/o inviare ad altri destinatari eventuali messaggi,del tipo "catene di Sant'Antonio", non sollecitati, che siano stati ricevuti, ed evitando di comunicare ad altri destinatari, in modo indiscriminato, il proprio indirizzo di posta elettronica o quello di colleghi.
- I Lavoratori non devono condurre attività commerciali di qualsiasi tipo a beneficio proprio e/o di terzi servendosi della Posta Elettronica dell'Istituzione Scolastica .
- E' fatto divieto, in ogni caso, di trasmettere a chiunque a mezzo Posta Elettronica Materiale pornografico, materiale fraudolento/illegale, gioco d'azzardo, materiale blasfemo o molesto/osceno.
  Il predetto divieto riguarda tanto il contenuto quanto gli allegati dei messaggi di Posta.
- I Lavoratori per adempiere il proprio dovere di diligenza e vigilanza nell'utilizzo dei beni e strumenti ad esso affidati hanno l'obbligo di impedire ad altri indebiti utilizzi della propria apparecchiatura informatica, non rilevando, al fine del difetto di responsabilità, il fatto che altri, in sua assenza, abbia potuto usare la postazione lavorativa. In difetto, il comportamento si configura come negligente, inescusabile e gravemente colposo.

Per evitare ogni interferenza con la sfera privata del personale docente e ATA, qualunque comunicazione di interesse amministrativo o di lavoro dovrà avvenire per mezzo delle caselle istituzionali.
La consultazione della posta elettronica da parte dei dipendenti può quindi riguardare:

- caselle personali: su dominio ***istruzione.it***, messa a disposizione da parte del MIUR (e/o casella personale privata, su altro dominio)
- caselle istituzionali di lavoro comunicato dal Responsabile del Interno del Trattamento dei Dasti

A. Uso delle Caselle Personali

Il personale può consultare in orario di servizio caselle personali per motivi legati alla propria attività lavorativa. La gestione deve essere effettuata tramite servizi di "webmail": non è consentito configurare su computer dell'Istituto appositi programmi tipo Outlook o Thunderbird per gestire le proprie caselle personali (anche per garantire al dipendente la dovuta riservatezza).
Nell'uso di caselle personali all'interno della scuola, al dipendente non è comunque consentito:

- inviare messaggi dannosi, di tipo offensivo o sconveniente, come ad esempio, a titolo non esaustivo, messaggi che riportino contenuti o commenti oltraggiosi su argomenti sessuali, razziali, religiosi, politici, ecc. e comunque ogni altra tipologia di messaggio che possa arrecare danno alla reputazione della Scuola o del MIUR;
- l'uso del servizio di posta elettronica a scopi commerciali o di profitto personale e per attività illegali;
- utilizzare tecniche di "mail spamming" cioè di invio massiccio di comunicazioni a liste di distribuzione extra lavorative o azioni equivalenti.

B. Uso delle Caselle Istituzionali Di Lavoro

Le caselle istituzionali sono gestite dagli incaricati del trattamento dei Dati in base ai compiti loro assegnati. In caso di assenza dell'incaricato abituale, questo potrà essere sostituito da altro personale, in base all'organizzazione interna del lavoro disposta da D.S. o D.S.G.A.: quindi tali caselle devono essere utilizzate solo a scopo lavorativo e **NON d**evono essere utilizzate come caselle personali.
Oltre alle disposizioni impartite per l'utilizzo delle caselle personali, si aggiungono le seguenti disposizioni:

- Evitare di aprire messaggi provenienti da mittenti sconosciuti e che contengono allegati sospetti (file con estensione .exe, .scr, .pif, .bat, .cmd,.....). In caso di dubbio consultare un tecnico.
- Nel caso in cui si debba inviare un documento all'esterno dell'Istituto, se non specificamente destinato alla modifica, è preferibile utilizzare il formato *.pdf.
- Evitare che la diffusione incontrollata di "Catene di Sant'Antonio" (messaggi a diffusione capillare e moltiplicata) limiti l'efficienza del sistema di posta.
- Evitare di inviare allegati di dimensioni eccessive (se necessario usare formati compressi come *.zip, *.rar, ...)
- L'iscrizione a "*mailing list*" esterne è concessa solo per motivi professionali, prima di iscriversi occorre verificare in anticipo se il sito è affidabile.
- La casella di posta deve essere mantenuta in ordine.

Art. 12 I Controlli

1. Qualsiasi forma di controllo venga effettuata, deve essere strettamente necessaria per il Titolare del Trattamento, in relazione a scopi determinati e per il perseguimento di finalità organizzative, produttive e di sicurezza ha facoltà di effettuare qualsiasi forma di controllo necessaria;
2. Nell'eventualità di anomalie riscontrate nell'utilizzo da parte dei Lavoratori degli strumenti di lavoro messi a disposizione dalla Istituzione Scolastica, il Titolare

del Trattamento, unitamente al DPO, effettua una prima segnalazione, nella quale non può essere indicato alcun nominativo di Lavoratori, indicando al Responsabile interno o esterno del trattamento il computer nel quale è stata rilevata l'anomalia. Quest'ultimo provvede, a sua volta, ad inviare un avviso generalizzato diretto a tutti i Lavoratori appartenenti alla sua Struttura, nel quale evidenzia l'utilizzo irregolare degli strumenti messi a disposizione dalla Istituzione Scolastica, invitando i Lavoratori ad attenersi scrupolosamente ai compiti assegnati e alle istruzioni impartite.

3. Se l'avviso generalizzato di cui al punto 2 non produce effetto e l'anomalia rilevata persiste, il Titolare del trattamento, il DPO e l'Amministratore di Sistema, procedono ad un controllo su base individuale e nominativa, a seguito del quale il Titolare effettua una seconda segnalazione al Responsabile interno indicando l'area presso la quale è inserito il Lavoratore interessato dalle verifiche.
4. Il Titolare del Trattamento nelle funzioni di Dirigente Scolastico, effettuate le necessarie verifiche, attiverà direttamente il procedimento disciplinare nei confronti del Lavoratore ai sensi qualora il fatto sia di gravità tale da comportare una sanzione tra quelle di sua competenza.
   L'Amministrazione è tenuta alla riservatezza in tutte le fasi di accertamento dei fatti;
5. La rilevazione delle anomalie e delle verifiche tecniche di cui ai precedenti punti 2 e 3, è a cura dell'Amministratore di Sistema. Responsabile dei successivi e consequenziali provvedimenti è il Dirigente Scolastico.
6. L'Istituzione Scolastica, nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del Lavoratore, procede, in caso di anomalie, alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet , della Posta Elettronica e del telefono fisso nonché dei files con il dettaglio dei numeri chiamati totalmente "in chiaro" delle telefonate per il tempo strettamente necessario alla soluzione delle suddette anomalie.

Art. 13: Obbligatorietà e Sanzioni

1. È fatto obbligo a tutti i Lavoratori di osservare le disposizioni portate a conoscenza con il presente Regolamento. La omessa osservanza o la violazione delle regole contenute nel Regolamento è perseguibile con tutte le azioni civili (eventuale risarcimento del danno cagionato).
2. e penali previste dalla legge, nonché con i provvedimenti disciplinari, in conformità a quanto previsto dalle disposizioni normative e contrattuali vigenti per il personale scolastico Il codice di comportamento ed il codice disciplinare sono consultabili nel sito internet della Istituzione Scolastica.

Art. 14 Gestione della casella di Posta Elettronica di un Lavoratore cessato dal servizio

1. In caso di cessazione del rapporto di lavoro l'account di Posta Elettronica del Lavoratore è prontamente bloccato e la sua casella di Posta Elettronica non è più funzionante.
2. I mittenti di email inviate all'indirizzo e-mail bloccato vengono automaticamente informati che l'indirizzo del destinatario è estinto al momento della cancellazione dell'account.

Art. 15: Esercizio dei diritti

I Lavoratori hanno ricevuto informativa sulle modalità di esercizio dei diritti quali previsti dal DGPR 679/2016 in assonanza col D.Lvo 101/2018**.** Comunque:

1. I dati personali inerenti i Lavoratori non possono essere portati a conoscenza di terzi non autorizzati.
2. L'Istituzione Scolastica nell'ambito di procedimenti disciplinari e/o di procedimenti penali di cui all'art. 12 del presente Regolamento e nel rispetto del principio di protezione dei dati personali e del divieto di controllo a distanza del Lavoratore, procede alla conservazione delle "registrazioni a giornale" (log file) relative all'utilizzazione di Internet e/o della Posta Elettronica e/o dei files delle telefonate fino alla conclusione dei relativi procedimenti.
3. .Il presente documento viene portato a conoscenza di tutti i Lavoratori mediante pubblicazione nei sito internet.

Art. 16 Aggiornamento e Revisione

Tutti gli utenti possono proporre, quando ritenuto necessario, integrazioni al presente Regolamento. Le proposte verranno esaminate dal Titolare del Trattamento e dal DPO. Il presente Regolamento è soggetto a revisione con frequenza annuale.

In …. così dato il……..

ALLEGATO n° 4

LE SANZIONI

A.LE SANZIONI PREVISTE DAL GDPR 679/2016

(le slide's che seguono sono tratte dal corso di formazione tenuto dal DPO Dr. Giuseppe Renato Croce tal titolo " Le sanzioni previste dal GDPR 679/2016 e dal D.Lvo 101/2018")

SANZIONI DI CARATTERE ECONOMICO
1° livello

Le sanzioni applicabili, individuate nel Regolamento, sono pari a:

- **fino ad Euro 10.000.000,00, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni degli obblighi relativi a: minori, obblighi del Titolare e Responsabile, obblighi dell'organismo di certificazione, obblighi dell'organismo di controllo;**
- **fino ad Euro 20.000.000,00, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per le violazioni degli obblighi relativi a: principi di base del trattamento, comprese le condizioni relative al consenso, diritti degli interessati, trasferimento dati a paese extra UE, obblighi imposti dagli stati membri per specifiche categorie - anche in ambito lavorativo — l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi di dati dell'autorità di controllo.**

SANZIONI DI CARATTERE ECONOMICO

1° livello

SANZIONE AMMINISTRATIVA ECONOMICA	NORMA	VIOLAZIONE
Fino a 10.000.000 EUR o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. 8	Verifica che il consenso del trattamento sia prestato o autorizzato dal titolare della responsabilità genitoriale nel caso di offerta diretta di servizi della società dell'informazione a minori di età inferiore ai 16 anni.
	Art. 11	Obbligo di non conservazione, acquisizione o trattamento di informazioni per identificare l'Interessato se le finalità del trattamento non richiedono o non richiedono più l'identificazione dell'Interessato.
	Art. 25	Adozione di misure tecniche e organizzative atte ad attuare i principi di protezione dei dati, la tutela dei diritti degli Interessati e la garanzia che siano trattati, per impostazione predefinita, solo i dati necessari per ogni specifica finalità di trattamento (c.d. *privacy by design e by default).*
	Art. 28	Designazione del Responsabile del trattamento e rispetto ~ obblighi e compiti posti a carico del Responsabile.

SANZIONI DI CARATTERE ECONOMICO

1° livello

SANZIONE AMMINISTRATIVA ECONOMICA	NORMA	OBBLIGO VIOLATO
Fino a 10.000.000 EUR o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. 30	Tenuta dei Registri delle attività di trattamento.
	Art. 32	Adozione di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio
	Art. 33 e 34	Notifica delle violazioni all'Autorità di controllo
	Art. 35 e 36	Obbligo di procedere alla valutazione di impatto ed alla successiva consultazione, ove richiesto dal Regolamento.
	Art. 37 e 39	Prescrizioni in tema di designazione del Responsabile della protezione dei dati *(Data Protection Officer)*.

SANZIONI DI CARATTERE ECONOMICO

2° livello

SANZIONE AMMINISTRATIVA ECONOMICA	NORMA	OBBLIGO VIOLATO
Fino a 20.000.000 EUR o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. da 12 a 22	· Obblighi informativi nei confronti dell'Interessato. · Tutela dei diritti dell'Interessato (diritto d'accesso; di rettifica; all'oblio; di limitazione del trattamento; di notifica in caso di rettifica o cancellazione dei dati o limitazione del trattamento; alla portabilità dei dati; di opposizione; alla profilazione consenziente).
	Art. da 44 a 49	Obblighi connessi al trasferimento dei dati personali verso Paesi terzi o organizzazioni internazionali.
	Cap IX	Qualsiasi obbligo previsto dalle legislazioni degli Stati membri per specifiche situazioni di trattamento a norma del Capo IX del Regolamento.
	Art. 58	Rispetto di un ordine, di una limitazione di trattamento o di un ordine di sospensione di flussi di dati dell'Autorità di controllo o di un negato accesso ai sensi dell'Art, 58, par. I.

40

SANZIONI DI CARATTERE ECONOMICO

2° livello

SANZIONE AMMINISTRATIVA PECUNIARIA	NORMA	OBBLIGO VIOLATO
Fino a 20.000.000 EUR o, per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore	Art. 5	Rispetto dei principi applicabili al trattamento liceità, correttezza e trasparenza; limitazione delle finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.
	Art. 6	Rispetto delle condizioni di liceità del trattamento.
	Art. 7	· Dimostrazione della prestazione del consenso e del rispetto delle condizioni per il consenso. · Tutela del diritto dell'Interessato di revoca del consenso.
	Art. 9	Rispetto delle condizioni di liceità del trattamento di categorie particolari di dati personali.

SANZIONI CORRETTIVE/AVVERTIMENTI

Le sanzioni correttive sono connesse ai **poteri** dell'Autorità di controllo. consistono :

- **Rivolgere avvertimenti** al titolare del trattamento o al responsabile del trattamento sul fatto che i trattamenti previsti possono violare il GDPR
- **Rivolgere ammonimenti** al titolare e del trattamento o al responsabile del trattamento ove i trattamenti abbiano violato le disposizioni del GDPR
- **Ingiungere** al titolare del trattamento o al responsabile del trattamento **di soddisfare le richieste** dell'interessato di esercitare i relativi diritti
- **Ingiungere** al titolare o al responsabile del trattamento **di conformare i trattamenti alle disposizioni del GDPR**, anche specificando in che modo ed entro quale termine
- **Ingiungere** al titolare del trattamento **di comunicare all'interessato una violazione** dei dati personali
- **Imporre una limitazione** provvisoria o definitiva al trattamento, incluso il divieto di trattamento
- **Ordinare la rettifica, la cancellazione di dati personali o la limitazione del trattamento** e la notificazione di tali misure ai destinatari cui sono stati comunicati i dati personali
- **Revocare la certificazione** o ingiungere all'organismo di certificazione di ritirare la certificazione rilasciata a norma degli articoli 42 e 43, oppure ingiungere all'organismo di certificazione di non rilasciare la certificazione se i requisiti per la certificazione non sono o non sono più soddisfatti
- **Infliggere una sanzione amministrativa pecuniaria** in aggiunta alle presenti misure (v. sopra)
- **Ordinare la sospensione dei flussi** di dati verso un destinatario in un paese terzo o un'organizzazione internazionale

B.LE SANZIONI PREVISTE DAL D.LVO 101/2018

Modifiche alla parte III, titolo III, del decreto legislativo 30 giugno 2003, n. 196

1. Alla parte III, titolo III, del decreto legislativo 30 giugno 2003, n. 196, sono apportate le seguenti modificazioni:

a) l'articolo 166 e' sostituito dal seguente:

«***Art. 166*** ***(Criteri di applicazione delle sanzioni amministrative pecuniarie e procedimento per l'adozione dei provvedimenti correttivi e sanzionatori***).

- 1. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 4, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-quinquies, comma 2,2-quinquiesdecies, 92, comma 1, 93, comma 1, 123, comma 4, 128, 129,comma 2, e 132-ter. Alla medesima sanzione amministrativa e' soggetto colui che non effettua la valutazione di impatto di cui all'articolo 110, comma 1, primo periodo, ovvero non sottopone il programma di ricerca a consultazione preventiva del Garante a norma del terzo periodo del predetto comma.

2. Sono soggette alla sanzione amministrativa di cui all'articolo 83, paragrafo 5, del Regolamento le violazioni delle disposizioni di cui agli articoli 2-ter, 2-quinquies, comma 1, 2-sexies, 2-septies, comma 7, 2-octies, 2-terdecies, commi 1, 2, 3 e 4, 52, commi 4 e 5, 75, 78, 79, 80, 82, 92, comma 2, 93, commi 2 e 3, 96, 99, 100, commi 1, 2 e 4, 101, 105 commi 1, 2 e 4, 110-bis, commi 2 e 3, 111, 111-bis, 116, comma 1, 120, comma 2, 122, 123, commi 1, 2, 3 e 5, 124, 125, 126, 130, commi da 1 a 5, 131, 132, 132-bis, comma 2, 132-quater, 157, nonche' delle misure di garanzia, delle regole deontologiche di cui rispettivamente agli articoli 2-septies e 2-quater.

3. Il Garante e' l'organo competente ad adottare i provvedimenti correttivi di cui all'articolo 58, paragrafo 2, del Regolamento, nonche' ad irrogare le sanzioni di cui all'articolo 83 del medesimo Regolamento e di cui ai commi 1 e 2.

4. Il procedimento per l'adozione dei provvedimenti e delle sanzioni indicati al comma 4 puo' essere avviato, nei confronti sia di soggetti privati, sia di autorita' pubbliche ed organismi pubblici, a seguito di reclamo ai sensi dell'articolo 77 del Regolamento o di attivita' istruttoria d'iniziativa del Garante, nell'ambito dell'esercizio dei poteri d'indagine di cui all'articolo 58, paragrafo 1, del Regolamento, nonche' in relazione ad accessi, ispezioni e verifiche svolte in base a poteri di accertamento autonomi, ovvero delegati dal Garante.
5. L'Ufficio del Garante, quando ritiene che gli elementi acquisiti nel corso delle attivita' di cui al comma 5 configurino una o piu' violazioni indicate nel presente titolo e nell'articolo 83, paragrafi 4, 5 e 6, del Regolamento, avvia il procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 4 notificando al titolare o al responsabile del trattamento le presunte violazioni, nel rispetto delle garanzie previste dal Regolamento di cui al comma 10, salvo che la previa notifica della contestazione non risulti incompatibile con la natura e le finalita' del provvedimento da adottare.
6. Entro trenta giorni dal ricevimento della comunicazione di cui al comma 6, il contravventore puo' inviare al Garante scritti difensivi o documenti e puo' chiedere di essere sentito dalla medesima autorita'.
7. Nell'adozione dei provvedimenti sanzionatori nei casi di cui al comma 4 si osservano, in quanto applicabili, gli articoli da 1 a 9, da 18 a 22 e da 24 a 28 della legge 24 novembre 1981, n. 689; nei medesimi casi puo' essere applicata la sanzione amministrativa accessoria della pubblicazione dell'ordinanza-ingiunzione, per intero o per estratto, sul sito internet del Garante. I proventi delle sanzioni, nella misura del cinquanta per cento del totale annuo, sono riassegnati al fondo di cui all'articolo 156, comma 8, per essere destinati alle specifiche attivita' di sensibilizzazione e di ispezione nonche' di attuazione del Regolamento svolte dal Garante.
8. Entro il termine di cui all'articolo 10, comma 3, del decreto legislativo n. 150 del 2011 previsto per la proposizione del ricorso, il trasgressore e gli obbligati in solido possono definire la controversia adeguandosi alle prescrizioni del Garante, ove impartite, e mediante il pagamento di un importo pari alla meta' della sanzione irrogata.
9. Nel rispetto dell'articolo 58, paragrafo 4, del Regolamento, con proprio regolamento pubblicato nella Gazzetta Ufficiale della Repubblica italiana, il Garante definisce le modalita' del procedimento per l'adozione dei provvedimenti e delle sanzioni di cui al comma 4 ed i relativi termini, in conformita' ai principi della

piena conoscenza degli atti istruttori, del contraddittorio, della verbalizzazione, nonche' della distinzione tra funzioni istruttorie e funzioni decisorie rispetto all'irrogazione della sanzione.
10. Le disposizioni relative a sanzioni amministrative previste dal presente codice e dall'articolo 83 del Regolamento non si applicano in relazione ai trattamenti svolti in ambito giudiziario.».
b) l'articolo 167 e' sostituito dal seguente:

«Art. 167 (Trattamento illecito di dati).

- 1. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, operando in violazione di quanto disposto dagli articoli 123, 126 e 130 o dal provvedimento di cui all'articolo 129 arreca nocumento all'interessato, e' punito con la reclusione da sei mesi a un anno e sei mesi.
2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trattamento dei dati personali di cui agli articoli 9 e 10 del Regolamento in violazione delle disposizioni di cui agli articoli 2-sexies e 2-octies, o delle misure di garanzia di cui all'articolo 2-septies ovvero operando in violazione delle misure adottate ai sensi dell'articolo 2-quinquiesdecies arreca nocumento all'interessato, e' punito con la reclusione da uno a tre anni.
3. Salvo che il fatto costituisca piu' grave reato, la pena di cui al comma 2 si applica altresi' a chiunque, al fine di trarre per se' o per altri profitto ovvero di arrecare danno all'interessato, procedendo al trasferimento dei dati personali verso un paese terzo o un'organizzazione internazionale al di fuori dei casi consentiti ai sensi degli articoli 45, 46 o 49 del Regolamento, arreca nocumento all'interessato.
4. Il Pubblico ministero, quando ha notizia dei reati di cui ai commi 1, 2 e 3, ne informa senza ritardo il Garante.
5. Il Garante trasmette al pubblico ministero, con una relazione motivata, la documentazione raccolta nello svolgimento dell'attivita' di accertamento nel caso in cui emergano elementi che facciano presumere la esistenza di un reato. La trasmissione degli atti al pubblico ministero avviene al piu' tardi al termine dell'attivita' di

accertamento delle violazioni delle disposizioni di cui al presente decreto.
6. Quando per lo stesso fatto e' stata applicata a norma del presente codice o del Regolamento a carico dell'imputato o dell'ente una sanzione amministrativa pecuniaria dal Garante e questa e' stata riscossa, la pena e' diminuita.»;
c) dopo l'articolo 167, sono inseriti i seguenti:

Art. 167-bis ***(Comunicazione e diffusione illecita di dati personali oggetto di trattamento su larga scala).***

- 1. Salvo che il fatto costituisca piu' grave reato, chiunque comunica o diffonde al fine di trarre profitto per se' o altri ovvero al fine di arrecare danno, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, in violazione degli articoli 2-ter, 2-sexies e 2-octies, e' punito con la reclusione da uno a sei anni.
2. Salvo che il fatto costituisca piu' grave reato, chiunque, al fine trarne profitto per se' o altri ovvero di arrecare danno, comunica o diffonde, senza consenso, un archivio automatizzato o una parte sostanziale di esso contenente dati personali oggetto di trattamento su larga scala, e' punito con la reclusione da uno a sei anni, quando il consenso dell'interessato e' richiesto per le operazioni di comunicazione e di diffusione.
3. Per i reati di cui ai commi 1 e 2, si applicano i commi 4, 5 e 6 dell'articolo 167.».
corrispondere gli importi indicati negli atti di cui al primo periodo del predetto comma entro sessanta giorni dalla scadenza del termine previsto dal comma 1.
4. Entro il termine di cui al comma 3, il contravventore che non

abbia provveduto al pagamento puo' produrre nuove memorie difensive. Il Garante, esaminate tali memorie, dispone l'archiviazione degli atti comunicandola all'organo che ha redatto il rapporto o, in alternativa, adotta specifica ordinanza-ingiunzione con la quale determina la somma dovuta per la violazione e ne ingiunge il pagamento, insieme con le spese, all'autore della violazione ed alle persone che vi sono obbligate solidalmente.

5. L'entrata in vigore del presente decreto determina l'interruzione del termine di prescrizione del diritto a riscuotere le somme dovute a norma del presente articolo, di cui all'art. 28 della legge 24 novembre 1981, n. 689.

d) gli allegati B e C.

ALLEGATO N° 5 LE NOMINE

- **atti di nomina del Responsabile interno del Trattamento dei Dati**
- **le istruzioni scritte comunicate agli incaricati (nominative o per classi omogenee) con le responsabilità connesse alle mansioni da ricoperte ciascuno**
- **istruzioni al custode delle credenziali. Dovranno altresì essere specificate le responsabilità connesse alle mansioni da ciascuno ricoperte all'interno della struttura aziendale.**

ALLEGATO N° 6: ISTRUZIONI AI TECNICI PER L' ANALISI DEI RISCHI

ANALISI DELLA SITUAZIONE DELLA ISTITUZIONE SCOLASTICA
Ic Piazza Filattiera 84 Roma

1) Descrizione del Sistema Informatico

HARDWARE

HARDWARE: composto da server Lenovo con 16 Gb ram hdd da 1Tb – client ; n4 pc Hp i5 6Gen con windows 7 pro e n.4 pc Hp i5 7 gen con windows 10 pro

- Reti locali ed altri sistemi di collegamento di terminali gestita da Riuter in fibra-unità Swicth cisco catalist con n.3 vlan e firewall di gestione
- Unità di accesso per gli utenti (terminali, personal computer, workstations, stampanti, telefax)
- Collegamenti del sistema a apparecchiature di produzione o altri dispositivi di acquisizione dati a messo di multifunzione: Kyocera
- Dispositivi di connessione verso l'esterno, per singoli utenti o condivisi tra più utenti: nessuno

SOFTWARE

- Sistemi operativi utilizzati Windows server 2019 essential- Windows 7 pro e windows 11 Pro

- software antivirus Symantec endpoint protection 10 ut

- software di gestione backup Acronis server

- copie su nas Synology protetto e automatizzato per accensione e spegnimento

- - Applicazioni di tipo gestionale Axios software
- - Applicazioni di office automation Pacchetto Office Microsoft

- Applicazioni tecniche o grafiche (CAD/CAM, progettazione, ecc.) nessuno

- Sistemi di posta elettronica e strumenti di navigazione in Internet outlook-webmail-browser Crome

2) Analisi ed elenco dei dati personali

In riferimento alle applicazioni esistenti si deve determinare se esse trattano, anche potenzialmente dati personali secondo quanto previsto dal DGPR 679/2016 in correlazione col D.Lvo 101/2018

Particolare attenzione va posta riguardo all'utilizzo dei prodotti di office automation, data la libertà d'azione che tali prodotti concedono agli utenti sia riguardo al contenuto dei documenti generati, sia riguardo alla loro gestione.
E', altresì, opportuno illustrare anche eventuali applicazioni che, pur non riguardando dati personali, sono gestite mediante il sistema informatico.
E' opportuno, altresì, individuare ed elencare le *"**BANCHE DATI**"* realizzate con le specifiche applicazioni in uso (*ad es. alunni, personale scolastico ecc…)* e specificare le finalità di trattamento.
Analogamente dovrà essere effettuata l'analisi degli archivi cartacei.

3) Analisi ed elenco dei trattamenti di dati "particolari";

a) Trattamento con strumenti elettronici

Evidenziare la presenza di dati personali di tipo *"particolare"* (ex artt. 9 e 10 GDPR) all'interno del sistema informatico aziendale e soprattutto:

- I server e/o i sistemi su cui sono archiviati i dati particolari
- Le applicazione utilizzate per il trattamento
- Le finalità del trattamento
- Gli specifici tipi di dati particolari esistenti nel sistema ***(elencare le banche dati relative)***

b) Trattamento senza l'ausilio di strumenti elettronici

- Dislocazione fisica degli archivi
- Le finalità del trattamento
- Gli specifici tipi di dati particolari presenti negli archivi cartacei *(elencare le banche dati relative)*

4) Analisi dei rischi possibili e dei danni conseguenti

Si devono individuare ed elencare i possibili rischi cui è esposto il sistema informatico quali ad es.:

- Alterazione/danneggiamento accidentale o dolosa del sistema, dei programmi e/o dati
- Diffusione/comunicazione non autorizzata sia accidentale che dolosa
- Danneggiamento delle risorse informatiche per disastri naturali (incendi...)
- Accessi non autorizzati

- Sottrazione di elaboratori, programmi, supporti o dati
- Intrusioni dall'esterno nel sistema
- .....

Si devono altresì individuare i tipi di danni arrecabili ai dati personali quali ad es.:

- Distruzione dei dati
- Alterazione dei dati
- Trattamento/comunicazione/diffusione non autorizzata dei dati

A - MISURE DI SICUREZZA ADOTTATE O DA ADOTTARE

Debbono essere elencate le misure di sicurezza o realizzate nella realtà tecnologica ed organizzativa. In particolare andranno evidenziate:

❖ ***Misure per i trattamenti informatici***

- Definizione delle credenziali di autenticazione, individuate tra le seguenti tipologie:
  1. Codice identificativo, più parola chiave
  2. Dispositivo di autenticazione (*smart card e simili*), più eventuale parola chiave
- Modalità di attivazione, variazione e gestione delle credenziali
- Criteri di definizione dei profili di autorizzazione
- Attribuzione, revoca ed aggiornamento dei profili di autorizzazione
- Criteri di utilizzo e di aggiornamento dei programmi antivirus e dei programmi di antintrusione
- Aggiornamento dei programmi volti a prevenire vulnerabilità ed a correggerne i difetti (*software update*)

❖ ***Misure per i trattamenti cartacei***

- Procedure e modalità per l'organizzazione degli archivi cartacei ad accesso autorizzato
- Modalità di custodia dei dati particolari durante l'utilizzo
- Modalità di identificazione e registrazione degli accessi ai dati particolari dopo l'orario di chiusura

5) Criteri tecnici ed organizzativi per la protezione delle aree e dei locali e procedure di controllo per l'accesso

Evidenziare se sussistono una o più delle seguenti misure per la protezione fisica:

- Localizzazione e limitazioni all'accesso del data center (localizzazione del server)
- Dispositivi antintrusione (specifici per il data center o generali per tutto l'edificio/stabilimento)
- Dispositivi antincendio (estintori, manichette, impianti di rilevazione e/o spegnimento automatico)
- Sistemi di registrazione degli ingressi e di chiusura dei locali
- Presenza di un custode e/o di un servizio di vigilanza esterna
- Custodia in armadi o classificatori ad accesso autorizzato
- Modalità di custodia delle chiavi
- .....

6) Criteri e procedure per assicurare l'integrità e la disponibilità dei dati;

Evidenziare se sussistono una o più delle seguenti procedure:

- Criteri di definizione del salvataggio dei dati
- Procedure per l'esecuzione del backup
- Definizione delle tecniche e dei criteri di backup
- Procedure per la conservazione dei backup (utilizzo di casseforti od armadi ignifughi)
- Procedure per la verifica della registrazione dei backup
- Presenza di un responsabile per l'esecuzione e la verifica dei backup
- Procedura di sostituzione ed eliminazione dei dispositivi di conservazione obsoleti (cassette, nastri magnetici, supporti ottici)

7) Criteri e procedure per il ripristino dell'accesso ai dati (Piano di disaster recovery)

Evidenziare se sussistono una o più delle seguenti procedure:

- Criteri di definizione per il ripristino dei dati (*a seguito di distruzione o danneggiamento dei dati stessi e/o degli strumenti elettronici*)

- Identificazione degli incidenti “eccezionali” dei sistemi informatici
- Definizione di procedure che assicurino tempi certi di ripristino dei sistemi
- Verifica periodica delle procedure attivate
- Definizione di una *policy* di business continuity

8) ***Criteri per garantire la predisposizione delle misure nel caso di trattamenti affidati all’esterno della struttura aziendale***

Evidenziare se sussistono la seguente misura :

- Definizione di una corretta applicazione delle misure di sicurezza da parte di responsabili esterni di trattamento relativi alla gestione di dati particolari;

9) **Eventuali altre misure**

Evidenziare se sussistono altre misure oltre quelle indicate nei punti 5 e 6

ALLEGATO 7: I CONTROLLI E LA TEMPISTICA

A. Trattamento con Strumenti Elettronici

MISURE DA VERIFICARE	**DESCRIZIONE MISURA**	**Tipologia dei dati**
Credenziali di autenticazione	disattivazione in caso di mancato utilizzo dei medesimi per un periodo superiore ai 6 mesi	
Credenziali di autenticazione	disattivazione in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali	
Codice per l'identificazione	una volta assegnato, non può essere assegnato ad altri incaricati	
Parola chiave	per il trattamento di dati personali deve essere modificata ogni sei mesi	
Parola chiave	per il trattamento di dati particolari deve essere modificata ogni tre mesi	Dati Particolari
Profili di autorizzazione	possono essere individuati per singolo incaricato o per classi omogenee di incaricati	
Profili di autorizzazione	verificare la sussistenza delle condizioni per la conservazione dei profili di autorizzazione	
Lista degli incaricati autorizzati	può essere redatta anche per classi omogenee di incarico	

Antivirus	efficacia ed aggiornamento sono verificati con cadenza almeno semestrale.	
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici	
Patch o programmi update	Programmi per elaboratore volti a correggere difetti e prevenire la vulnerabilità degli strumenti elettronici	Dati Particolari
Backup	salvataggio dei dati con frequenza settimanale	
Ripristino accesso dati	Ripristino accesso dati in caso di danneggiamento degli stessi o degli strumenti elettronici	Dati Particolari
Sistemi antintrusione	protezione contro l'accesso abusivo nel caso di trattamento di dati sensibili	
Custodia dei supporti rimovibili di memorizzazione	istruzioni organizzative e tecniche per la loro custodia e utilizzo	
Riutilizzo dei supporti di memorizzazione	se non utilizzati devono essere distrutti o resi inutilizzabili, controllo sulla non recuperabilità delle informazioni	

	precedentemente contenute	

B. Trattamento senza Strumenti Elettronici

MISURE DA VERIFICARE	DESCRIZIONE MISURA	Tipologia dei dati	CADENZA
Istruzioni scritte	Finalizzate al controllo e custodia dei documenti		sempre
Profili di autorizzazione	Individuazione dell'ambito del trattamento consentito agli incaricati, individuati anche per classi omogenee		1 anno
Procedure di controllo e custodia	Al fine di non consentire l'accesso a persone prive di autorizzazione	Dati Particolari	sempre
Accesso controllato agli archivi	Le persone ammesse dopo l'orario di chiusura devono essere identificate e registrate	Dati Particolari	sempre
Autorizzazione preventiva all'accesso	qualora gli archivi non siano dotati di strumenti elettronici per il controllo degli accessi o di incaricati alla vigilanza	Dati Particolari	sempre