SISTEMA PRIVACY

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

C.M.: TPIS02200A

C.F.: 93066580817

VIA CESARO', 36 - 91016 ERICE (TP)

Fonti Normative:
Codice della Privacy - D.Lgs. 196/2003
Regolamento Europeo UE 2016/679

Data di Creazione: 15.05.2018
Ultimo aggiornamento: 15.05.2018

INTRODUZIONE

Il Regolamento Generale sulla Protezione Dati (RGPD) - UE 2016/679

Il Regolamento UE 2016/679 emanato il 27 aprile 2016 stabilisce le regole valide in tutti i paesi dell'Unione Europea in materia di dati personali, senza necessità di leggi nazionali di recepimento. Il Regolamento Europeo sulla Protezione dei Dati, rispetto alla precedente normativa, introduce nuove modalità di trattamento e sicurezza dei dati che tengano conto di ogni aspetto: tecnico, organizzativo e procedurale, con un approccio basato sui rischi reali ed effettivi della propria attività.

Principali novità della normativa

***Accountability**:* Il principio del accountability richiede che il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR. E' l'approccio basato sulla valutazione del rischio che premia i soggetti più responsabili.

***Privacy by default e by design**:* Con la terminologia by default e by design si intende indicare la tutela dei dati personali impostata come impostazione predefinita (di default) e pensata fin dalla progettazione di prodotti e servizi (design): l'intento è quello di prevenire e non correggere. L'attenta valutazione d'impatto e di rischio, permetterà all'Azienda di individuare potenziali rischi e adottare adeguate misure sin dai primi processi di progettazione ed implementazione dei sistemi.

***Registro delle attività di trattamento**:* Con il Regolamento UE 2016/679, il titolare deve tenere un registro delle attività svolte sotto la propria responsabilità, messo su richiesta a disposizione dell'Autorità di controllo. In questo registro, fra le altre informazioni, devono essere riportate le misure di sicurezza tecniche ed organizzative adottate.

***Valutazione d'impatto sulla Protezione dei dati**:* Il titolare prima di procedere con il trattamento è tenuto ad effettuare una valutazione di impatto: sulla medesima dovranno essere evidenziati anche i rischi per gli interessati e le misure previste per affrontarli, descrivendo le misure di sicurezza adottate per proteggere i diritti e gli interessi legittimi degli interessati. Il titolare procede a un riesame per valutare se il trattamento dei dati sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio.

***Notifica di una violazione di dati personali**:* Tutti i titolari del trattamento dovranno notificare e documentare le violazioni di dati personali all'autorità Garante entro 72 ore dal momento in cui se ne viene a conoscenza. La notifica deve descrivere la natura della violazione, le probabili conseguenze e le misure adottate per porre rimedio alla violazione.

Il RGPD è pienamente operativo dal 25 maggio 2018.

REGISTRO DEI TRATTAMENTI DEL TITOLARE

Identificazione del trattamento				Soggetti	Finalità del trattamento	Trasferimenti al di fuori dell'UE	Dati sensibili
Nome	N ° REF	Data di creazione	Ultimo aggiornamento	Titolare del trattamento	Scopo principale	Sì / No	Sì / No
T1 - ALUNNI/GENITORI	11	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Istruzione ed assistenza scolastica	No	Si
T2 - ALUNNI/GENITORI	12	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Istruzione ed assistenza scolastica	No	Si
T3 - PERSONALE DIPENDENTE	13	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Trattamento giuridico ed economico del personale. Gestione del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Formazione professionale, Adempimento di obblighi fiscali e contabili. Adempimenti connessi	No	Si

T4 - COLLABORAZIONI PROFESSIONALI	14	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Trattamento dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri argo¬menti connessi alla categoria	No	Si
T5 - Fornitori Beni e servizi: acquisti, affitti, vendite	15	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Adempimento di obblighi fiscali e contabili, gestione dei fornitori/esperti/consulenti (beni e servizi).	No	Si
T6 - Gestione finanziaria e del bilancio	16	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Predisposizione del Bilancio Preventivo e del Conto Consuntivo. Loro trasmissione per via telematica. Gestione degli atti connessi al bilancio: mandati, ordinativi di pagamento anche informatici, reversali, rapporti con l'Istituto Cassiere e varie	No	Si
T7 - Gestione Istituzionale/ Protocollo/Posta	17	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Registrazione e cronologico dei documenti in arrivo ed in uscita dalla Scuola	No	Si
T8 - Archivio Delibere C.d.I., G.E., archivio verbali C.d.C. e C.d.D.	18	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Trattamento di tutti i dati della categoria delibere e verbali	No	Si
T9 - Gestione documenti cartacei dislocati lontano dalla segreteria	19	15/05/2018	15/05/2018	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	Gestione documenti cartacei dislocati lontano dalla segreteria. I documenti vengono prelevati dai locali di archivio per essere portati al personale di Segreteria per le necessarie lavorazioni e sviluppo pratiche.	No	Si

Descrizione del trattamento	
Nome / sigla	T1 - ALUNNI/GENITORI
No. / REF	11
Descrizione del Trattamento	Istruzione ed assistenza scolastica Trattamento dati alunni per la didattica e le altre attività correlate Trattamento dati alunni per le attività integrative e complementari
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Istruzione ed assistenza scolastica

Misure di sicurezza	
Misure di sicurezza tecniche	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Categorie di dati personali	Descrizione	Durata del trattamento

Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Dati personali non particolari	20 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento
Altri dati particolari	Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305.	20 Anni

Categorie di persone interessate	
Categoria	Alunni Frequentanti e/o diplomati e loro genitori.

Destinatari	Tipo di destinatari
Destinatario 1	Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze armate, Forze di polizia, Uffici giudiziari, Enti

Descrizione del trattamento	
Nome / sigla	T2 - ALUNNI/GENITORI
No. / REF	12
Descrizione del Trattamento	Istruzione ed assistenza scolastica, dati alunni e loro famiglie per l'attività amministrativa, altre attività correlate, attività di supporto alla didattica, attività integrative e complementari, assicurazione, infortuni, applicazione D.Lgs 81/2008.
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Istruzione ed assistenza scolastica

Misure di sicurezza	
Misure di sicurezza tecniche	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Categorie di dati personali	Descrizione	Durata del trattamento
Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Dati personali non particolari	20 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento
Altri dati particolari	Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305.	20 Anni

Categorie di persone interessate	
Categoria	Alunni Frequentanti e/o diplomati e loro genitori.

Destinatari	Tipo di destinatari
Destinatario 1	Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze armate, Forze di polizia, Uffici giudiziari, Enti

Descrizione del trattamento	
Nome / sigla	T3 - PERSONALE DIPENDENTE
No. / REF	13
Descrizione del Trattamento	Trattamento giuridico ed economico del personale, Gestione del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Formazione professionale, Adempimento di obblighi fiscali e contabili, Adempimenti connessi
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Trattamento giuridico ed economico del personale. Gestione del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Formazione professionale, Adempimento di obblighi fiscali e contabili. Adempimenti connessi

Misure di sicurezza	
Misure di sicurezza tecniche	Per trattamenti effettuati in adempimento di un obbligo legale, l’Autorità Garante ritiene che potranno restare in vigore le misure di sicurezza di cui all’allegato B.
Misure di sicurezza organizzative	L'incaricato del trattamento presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che assicurano la sicurezza del trattamento.

Categorie di dati personali	Descrizione	Durata del trattamento

Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Adesione a sindacati o organizzazione a carattere sindacale. Stato di salute, Informazioni concernenti i provvedimenti giudiziari. Codice fiscale ed altri numeri di identificazione personale, Nominativo indirizzo o altri elementi.	20 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento
Altri dati particolari	Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305.	20 Anni

Categorie di persone interessate	
Categoria	Personale interno alla scuola Docenti e ATA

Destinatari	Tipo di destinatari
Destinatario 1	Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze armate, Forze di polizia, Uffici giudiziari. Enti

Descrizione del trattamento	
Nome / sigla	T4 - COLLABORAZIONI PROFESSIONALI
No. / REF	14
Descrizione del Trattamento	Trattamento dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri argo¬menti connessi alla categoria
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Trattamento dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri argo¬menti connessi alla categoria

Misure di sicurezza	
Misure di sicurezza tecniche	Per trattamenti effettuati in adempimento di un obbligo legale, l’Autorità Garante ritiene che potranno restare in vigore le misure di sicurezza di cui all’allegato B.
Misure di sicurezza organizzative	L'incaricato del trattamento presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che assicurano la sicurezza del trattamento.

Categorie di dati personali	Descrizione	Durata del trattamento

Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Codice fiscale ed altri numeri di identificazione personale, Nominativo indirizzo o altri elementi di identificazione personale (nome. Cognome, età. sesso, luogo e data di nascita: indirizzo privato, indirizzo di lavoro, Tel., Solvibilità, Assicur.	20 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento
Appartenenza sindacale		20 Anni
Dati relativi alle condanne penali e reati o connesse misure di sicurezza		20 Anni
Origine razziale o etnica		20 Anni

Categorie di persone interessate	
Categoria	Consulenti esterni, Collaboratori professionali

Destinatari	Tipo di destinatari
Destinatario 1	Organi costituzionali o di rilievo costituzionale. Uffici giudiziari. Banche ed istituti di credito

Descrizione del trattamento	
Nome / sigla	T5 - Fornitori Beni e servizi: acquisti, affitti, vendite
No. / REF	15
Descrizione del Trattamento	Trattamento dati amministrativi, fiscali e tutti gli altri argomenti connessi alla categoria
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Adempimento di obblighi fiscali e contabili, gestione dei fornitori/esperti/consulenti (beni e servizi).

Misure di sicurezza	
Misure di sicurezza tecniche	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Categorie di dati personali	Descrizione	Durata del trattamento
Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Dati personali non particolari	10 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento

Altri dati particolari	Eventuali altri dati particolari necessari per la gestione del rapporto.	10 Anni

Categorie di persone interessate	
Categoria	Fornitori

Destinatari	Tipo di destinatari
Destinatario 1	Azienda titolare, Altri soggetti legati da un contratto di servizio all'azienda titolare

Descrizione del trattamento	
Nome / sigla	T6 - Gestione finanziaria e del bilancio
No. / REF	16
Descrizione del Trattamento	Trattamento dati connessi alla gestione del bilancio e tutti gli argomenti connessi, compresi i rapporti con le banche
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Predisposizione del Bilancio Preventivo e del Conto Consuntivo. Loro trasmissione per via telematica. Gestione degli atti connessi al bilancio: mandati, ordinativi di pagamento anche informatici, reversali, rapporti con l'Istituto Cassiere e varie

Misure di sicurezza	
Misure di sicurezza tecniche	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Categorie di dati personali	Descrizione	Durata del trattamento
Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Dati personali non particolari	10 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento
Altri dati particolari	Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305.	10 Anni

Categorie di persone interessate	
Categoria	Fornitori, Banche, Dipendenti e Collaboratori

Destinatari	Tipo di destinatari
Destinatario 1	Solo azienda titolare, Altri soggetti legati da un contratto di servizio all'azienda titolare

Descrizione del trattamento	
Nome / sigla	T7 - Gestione Istituzionale/ Protocollo/Posta
No. / REF	17
Descrizione del Trattamento	Trattamento di tutta la documentazione in arrivo ed in uscita dall'Istituto.
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Registrazione e cronologico dei documenti in arrivo ed in uscita dalla Scuola

Misure di sicurezza	
Misure di sicurezza tecniche	Per trattamenti effettuati in adempimento di un obbligo legale, l’Autorità Garante ritiene che potranno restare in vigore le misure di sicurezza di cui all’allegato B.
Misure di sicurezza organizzative	L'incaricato del trattamento presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che assicurano la sicurezza del trattamento.

Categorie di dati personali	Descrizione	Durata del trattamento
Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Dati personali inerenti alla corrispondenza in arrivo ed in uscita dal Protocollo scolastico.	20 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento

Altri dati particolari	Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305.	20 Anni

Categorie di persone interessate	
Categoria	Tutti gli stakeholder della scuola

Destinatari	Tipo di destinatari
Destinatario 1	Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze armate, Forze di polizia, Uffici giudiziari. Enti

Descrizione del trattamento	
Nome / sigla	T8 - Archivio Delibere C.d.I., G.E., archivio verbali C.d.C. e C.d.D.
No. / REF	18
Descrizione del Trattamento	Archivio Delibere C.d.I., G.E., archivio verbali C.d.C. e C.d.D.
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Trattamento di tutti i dati della categoria delibere e verbali

Misure di sicurezza	
Misure di sicurezza tecniche	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Categorie di dati personali	Descrizione	Durata del trattamento
Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Dati personali non particolari	20 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento

Altri dati particolari	Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305.	20 Anni

Categorie di persone interessate	
Categoria	Dipendenti e Collaboratori, Alunni e familiari

Destinatari	Tipo di destinatari
Destinatario 1	Solo azienda titolare, Altri soggetti legati da un contratto di servizio all'azienda titolare

Descrizione del trattamento	
Nome / sigla	T9 - Gestione documenti cartacei dislocati lontano dalla segreteria
No. / REF	19
Descrizione del Trattamento	Gestione documenti cartacei dislocati lontano dalla segreteria
Data di creazione	15/05/2018
Ultimo aggiornamento	15/05/2018

Soggetti	Nome	Indirizzo	CAP	Città	Nazione	Telefono
Titolare al trattamento	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”	VIA CESARO', 36	91016	ERICE (TP)	Italia	0923.569559
Responsabile della protezione dati	BARRACO NATALE SALVATORE	VIA SPALTI 52	91100	Trapani (TP)	Italia	3289485541

Finalità del trattamento effettuato	
Finalità principale	Gestione documenti cartacei dislocati lontano dalla segreteria. I documenti vengono prelevati dai locali di archivio per essere portati al personale di Segreteria per le necessarie lavorazioni e sviluppo pratiche.

Misure di sicurezza	
Misure di sicurezza tecniche	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati.

Categorie di dati personali	Descrizione	Durata del trattamento
Dati personali non particolari (identificativi, contabili, finanziari, etc.)	Dati personali non particolari	20 Anni

Categorie di dati art. 9 e 10 RGPD	Descrizione	Durata del trattamento

Altri dati particolari	Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305.	20 Anni

Categorie di persone interessate	
Categoria	Dipendenti e Collaboratori, Fornitori, Alunni e loro genitori.

Destinatari	Tipo di destinatari
Destinatario 1	Solo azienda titolare, Altri soggetti legati da un contratto di servizio all'azienda titolare

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T1 - ALUNNI/GENITORI
Descrizione	Istruzione ed assistenza scolastica Trattamento dati alunni per la didattica e le altre attività correlate Trattamento dati alunni per le attività integrative e complementari
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018

Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta

Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018

Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	16/05/2018
Nome Trattamento	T2 - ALUNNI/GENITORI
Descrizione	Istruzione ed assistenza scolastica, dati alunni e loro famiglie per l'attività amministrativa, altre attività correlate, attività di supporto alla didattica, attività integrative e complementari, assicurazione, infortuni, applicazione D.Lgs 81/2008.
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018

Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta

Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018

Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T3 - PERSONALE DIPENDENTE
Descrizione	Trattamento giuridico ed economico del personale, Gestione del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Formazione professionale, Adempimento di obblighi fiscali e contabili, Adempimenti connessi
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018

Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta

Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018

Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T5 - Fornitori Beni e servizi: acquisti, affitti, vendite
Descrizione	Trattamento dati amministrativi, fiscali e tutti gli altri argomenti connessi alla categoria
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018

Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta

Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018

Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T4 - COLLABORAZIONI PROFESSIONALI
Descrizione	Trattamento dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri argo¬menti connessi alla categoria
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018

Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta

Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018

Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T6 - Gestione finanziaria e del bilancio
Descrizione	Trattamento dati connessi alla gestione del bilancio e tutti gli argomenti connessi, compresi i rapporti con le banche
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 2	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 3	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 8	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 9	Attacchi contro componenti Web
Data Rilevamento	15/05/2018

Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 10	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 11	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 12	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software

Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 13	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 14	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 15	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 16	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 17	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 18	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T7 - Gestione Istituzionale/ Protocollo/Posta
Descrizione	Trattamento di tutta la documentazione in arrivo ed in uscita dall'Istituto.
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018

Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 11	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 12	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 13	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 14	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 15	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 16	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T8 - Archivio Delibere C.d.I., G.E., archivio verbali C.d.C. e C.d.D.
Descrizione	Archivio Delibere C.d.I., G.E., archivio verbali C.d.C. e C.d.D.
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018

Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta

Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018

Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Analisi dei Rischi

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T9 - Gestione documenti cartacei dislocati lontano dalla segreteria
Descrizione	Gestione documenti cartacei dislocati lontano dalla segreteria
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 2	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 3	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 4	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 5	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 6	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 7	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T1 - ALUNNI/GENITORI
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Istruzione ed assistenza scolastica Trattamento dati alunni per la didattica e le altre attività correlate Trattamento dati alunni per le attività integrative e complementari
Categoria di dati trattati:		Descrizione: Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305. Tipologia: Altri dati particolari Durata: 20 Anni
		Descrizione: Dati personali non particolari Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 20 Anni
Categoria di soggetti interessati:		Alunni Frequentanti e/o diplomati e loro genitori.
Categoria di destinatari dei dati:		Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze armate, Forze di polizia, Uffici giudiziari, Enti
Finalità del trattamento:		Istruzione ed assistenza scolastica
Risorse interessate:	Hardware	Personal Computer ,Notebook, Tablet e Dispositivi Mobile,SERVER di Segreteria
	Software	Pacchetto OFFICE Microsoft,Software di Gestione delle Segreterie Didattiche (Client/Server),Piattaforma di Gestione del Registro Elettronico,Software di Gestione Documentale di Segreteria Digitale e Protocollo Web
	Persone	Unità Organizzativa "Corpo Insegnanti",Unità Organizzativa "Collaboratori Scolastici", DIRIGENTE SCOLASTICO PRO-TEMPORE,Unità Organizzativa "Intera Segreteria Scolastica"
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web

Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software

Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso

Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	16/05/2018
Nome Trattamento	T2 - ALUNNI/GENITORI
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Istruzione ed assistenza scolastica, dati alunni e loro famiglie per l'attività amministrativa, altre attività correlate, attività di supporto alla didattica, attività integrative e complementari, assicurazione, infortuni, applicazione D.Lgs 81/2008.
Categoria di dati trattati:		Descrizione: Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305. Tipologia: Altri dati particolari Durata: 20 Anni
		Descrizione: Dati personali non particolari Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 20 Anni
Categoria di soggetti interessati:		Alunni Frequentanti e/o diplomati e loro genitori.
Categoria di destinatari dei dati:		Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze armate, Forze di polizia, Uffici giudiziari, Enti
Finalità del trattamento:		Istruzione ed assistenza scolastica
Risorse interessate:	Hardware	Personal Computer ,Notebook, Tablet e Dispositivi Mobile,SERVER di Segreteria
	Software	Pacchetto OFFICE Microsoft,Software di Gestione Documentale di Segreteria Digitale e Protocollo Web,Piattaforma di Gestione del Registro Elettronico,Software di Gestione delle Segreterie Didattiche (Client/Server)
	Persone	Unità Organizzativa "Collaboratori Scolastici",Unità Organizzativa "Intera Segreteria Scolastica", DIRIGENTE SCOLASTICO PRO-TEMPORE
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018

Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T3 - PERSONALE DIPENDENTE
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Trattamento giuridico ed economico del personale, Gestione del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Formazione professionale, Adempimento di obblighi fiscali e contabili, Adempimenti connessi
Categoria di dati trattati:		Descrizione: Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305. Tipologia: Altri dati particolari Durata: 20 Anni
		Descrizione: Adesione a sindacati o organizzazione a carattere sindacale. Stato di salute, Informazioni concernenti i provvedimenti giudiziari. Codice fiscale ed altri numeri di identificazione personale, Nominativo indirizzo o altri elementi. Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 20 Anni
Categoria di soggetti interessati:		Personale interno alla scuola Docenti e ATA
Categoria di destinatari dei dati:		Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze armate, Forze di polizia, Uffici giudiziari. Enti
Finalità del trattamento:		Trattamento giuridico ed economico del personale. Gestione del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Formazione professionale, Adempimento di obblighi fiscali e contabili. Adempimenti connessi
Risorse interessate:	Hardware	Personal Computer ,Notebook, Tablet e Dispositivi Mobile,SERVER di Segreteria
	Software	Pacchetto OFFICE Microsoft,Software di Gestione delle Segreterie Didattiche (Client/Server),Software per la comunicazione telematica con agenzie fiscali,Software di Gestione Documentale di Segreteria Digitale e Protocollo Web
	Persone	DIRIGENTE SCOLASTICO PRO-TEMPORE,Unità Organizzativa "Intera Segreteria Scolastica",Unità Organizzativa "Collaboratori Scolastici"
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	Per trattamenti effettuati in adempimento di un obbligo legale, l'Autorità Garante ritiene che potranno restare in vigore le misure di sicurezza di cui all'allegato B.
Misure di sicurezza organizzative	L'incaricato del trattamento presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che assicurano la sicurezza del trattamento.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web

Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software

Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso

Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T4 - COLLABORAZIONI PROFESSIONALI
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Trattamento dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri argo¬menti connessi alla categoria
Categoria di dati trattati:		Tipologia: Appartenenza sindacale Durata: 20 Anni
		Tipologia: Dati relativi alle condanne penali e reati o connesse misure di sicurezza Durata: 20 Anni
		Tipologia: Origine razziale o etnica Durata: 20 Anni
		Descrizione: Codice fiscale ed altri numeri di identificazione personale, Nominativo indirizzo o altri elementi di identificazione personale (nome. Cognome, età. sesso, luogo e data di nascita: indirizzo privato, indirizzo di lavoro, Tel., Solvibilità, Assicur. Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 20 Anni
Categoria di soggetti interessati:		Consulenti esterni, Collaboratori professionali
Categoria di destinatari dei dati:		Organi costituzionali o di rilievo costituzionale. Uffici giudiziari. Banche ed istituti di credito
Finalità del trattamento:		Trattamento dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri argo¬menti connessi alla categoria
Risorse interessate:	Hardware	Personal Computer ,SERVER di Segreteria ,Notebook, Tablet e Dispositivi Mobile
	Software	Software di Gestione delle Segreterie Didattiche (Client/Server),Software per la comunicazione telematica con agenzie fiscali,Pacchetto OFFICE Microsoft,Software di Gestione Documentale di Segreteria Digitale e Protocollo Web
	Persone	DIRIGENTE SCOLASTICO PRO-TEMPORE,Unità Organizzativa "Intera Segreteria Scolastica",Unità Organizzativa "Collaboratori Scolastici"
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	Per trattamenti effettuati in adempimento di un obbligo legale, l'Autorità Garante ritiene che potranno restare in vigore le misure di sicurezza di cui all'allegato B.
Misure di sicurezza organizzative	L'incaricato del trattamento presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che assicurano la sicurezza del trattamento.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web

Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software

Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso

Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T5 - Fornitori Beni e servizi: acquisti, affitti, vendite
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Trattamento dati amministrativi, fiscali e tutti gli altri argomenti connessi alla categoria
Categoria di dati trattati:		Descrizione: Eventuali altri dati particolari necessari per la gestione del rapporto. Tipologia: Altri dati particolari Durata: 10 Anni
		Descrizione: Dati personali non particolari Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 10 Anni
Categoria di soggetti interessati:		Fornitori
Categoria di destinatari dei dati:		Azienda titolare, Altri soggetti legati da un contratto di servizio all'azienda titolare
Finalità del trattamento:		Adempimento di obblighi fiscali e contabili, gestione dei fornitori/esperti/consulenti (beni e servizi).
Risorse interessate:	Hardware	SERVER di Segreteria ,Personal Computer ,Notebook, Tablet e Dispositivi Mobile
	Software	Software per la comunicazione telematica con agenzie fiscali,Pacchetto OFFICE Microsoft,Software di Gestione delle Segreterie Didattiche (Client/Server),Software di Gestione Documentale di Segreteria Digitale e Protocollo Web
	Persone	Unità Organizzativa "Intera Segreteria Scolastica", DIRIGENTE SCOLASTICO PRO-TEMPORE,Unità Organizzativa "Collaboratori Scolastici"
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web

Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software

Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso

Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T6 - Gestione finanziaria e del bilancio
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Trattamento dati connessi alla gestione del bilancio e tutti gli argomenti connessi, compresi i rapporti con le banche
Categoria di dati trattati:		Descrizione: Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305. Tipologia: Altri dati particolari Durata: 10 Anni
		Descrizione: Dati personali non particolari Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 10 Anni
Categoria di soggetti interessati:		Fornitori, Banche, Dipendenti e Collaboratori
Categoria di destinatari dei dati:		Solo azienda titolare, Altri soggetti legati da un contratto di servizio all'azienda titolare
Finalità del trattamento:		Predisposizione del Bilancio Preventivo e del Conto Consuntivo. Loro trasmissione per via telematica. Gestione degli atti connessi al bilancio: mandati, ordinativi di pagamento anche informatici, reversali, rapporti con l'Istituto Cassiere e varie
Risorse interessate:	Hardware	Personal Computer ,Notebook, Tablet e Dispositivi Mobile,SERVER di Segreteria
	Software	Pacchetto OFFICE Microsoft,Software di Gestione Documentale di Segreteria Digitale e Protocollo Web,Software di Gestione delle Segreterie Didattiche (Client/Server),Software per la comunicazione telematica con agenzie fiscali
	Persone	Unità Organizzativa "Collaboratori Scolastici", DIRIGENTE SCOLASTICO PRO-TEMPORE,Unità Organizzativa "Intera Segreteria Scolastica"
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 2	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 3	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 8	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 9	Attacchi contro componenti Web

Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 10	Errata installazione hardware o errato uso
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 11	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 12	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati

Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 13	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 14	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 15	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 16	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 17	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 18	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T8 - Archivio Delibere C.d.I., G.E., archivio verbali C.d.C. e C.d.D.
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Archivio Delibere C.d.I., G.E., archivio verbali C.d.C. e C.d.D.
Categoria di dati trattati:		Descrizione: Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305. Tipologia: Altri dati particolari Durata: 20 Anni
		Descrizione: Dati personali non particolari Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 20 Anni
Categoria di soggetti interessati:		Dipendenti e Collaboratori, Alunni e familiari
Categoria di destinatari dei dati:		Solo azienda titolare, Altri soggetti legati da un contratto di servizio all'azienda titolare
Finalità del trattamento:		Trattamento di tutti i dati della categoria delibere e verbali
Risorse interessate:	Hardware	Personal Computer ,SERVER di Segreteria ,Notebook, Tablet e Dispositivi Mobile
	Software	Software di Gestione Documentale di Segreteria Digitale e Protocollo Web,Software di Gestione delle Segreterie Didattiche (Client/Server),Pacchetto OFFICE Microsoft
	Persone	Unità Organizzativa "Collaboratori Scolastici", DIRIGENTE SCOLASTICO PRO-TEMPORE,Unità Organizzativa "Intera Segreteria Scolastica",Unita Organizzativa "persone facenti parte degli organi collegiali"
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati e solo tramite l'utilizzo di password personali che vengono aggiornate periodicamente.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web

Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Minaccia 11	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software

Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 12	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 13	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 14	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 15	Errata installazione hardware o errato uso

Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 16	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 17	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 18	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T7 - Gestione Istituzionale/ Protocollo/Posta
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Trattamento di tutta la documentazione in arrivo ed in uscita dall'Istituto.
Categoria di dati trattati:		Descrizione: Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305. Tipologia: Altri dati particolari Durata: 20 Anni
		Descrizione: Dati personali inerenti alla corrispondenza in arrivo ed in uscita dal Protocollo scolastico. Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 20 Anni
Categoria di soggetti interessati:		Tutti gli stakeholder della scuola
Categoria di destinatari dei dati:		Organi costituzionali o di rilievo costituzionale, Organismi sanitari, personale medico e paramedico, Istituti e scuole di ogni ordine e grado ed università, Enti previdenziali ed assistenziali, Forze armate, Forze di polizia, Uffici giudiziari. Enti
Finalità del trattamento:		Registrazione e cronologico dei documenti in arrivo ed in uscita dalla Scuola
Risorse interessate:	Hardware	SERVER di Segreteria ,Personal Computer ,Notebook, Tablet e Dispositivi Mobile
	Software	Software per la comunicazione telematica con agenzie fiscali,Software di Gestione Documentale di Segreteria Digitale e Protocollo Web,Pacchetto OFFICE Microsoft,Software di Gestione delle Segreterie Didattiche (Client/Server)
	Persone	Unità Organizzativa "Intera Segreteria Scolastica",Unità Organizzativa "Collaboratori Scolastici", DIRIGENTE SCOLASTICO PRO-TEMPORE
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	Per trattamenti effettuati in adempimento di un obbligo legale, l'Autorità Garante ritiene che potranno restare in vigore le misure di sicurezza di cui all'allegato B.

Misure di sicurezza organizzative	L'incaricato del trattamento presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che assicurano la sicurezza del trattamento.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 2	MALWARE - Software creato allo scopo di introdursi in un computer senza autorizzazioni per trafugarne i dati o causare danni al sistema informatico su cui viene eseguito
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Adozione di misure antimalware applicate a tutti i canali di comunicazione da/verso l'esterno (server, infrastrutture di rete, personal computer e dispositivi mobili), Adozione di politiche di sicurezza per definire preventivamente a tutti i livelli le procedure da seguire nei casi di infezione (da quelli dirigenziali agli operativi, fino agli utenti finali), Aggiornamento regolare dei controlli di prevenzione dei malware e adeguamento degli stessi a nuovi metodi di attacco, Monitoraggio sistematico dei test antivirus, Utilizzo di tools per l'analisi dei malware nell'ambito di una gestione degli "incidenti" in grado di assicurare una risposta efficace
Rischio residuale:	No

Minaccia 3	Danneggiamento del disco fisso o del supporto di memorizzazione dei dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo

Contromisure adottate:	Copia di backup dei dati
Rischio residuale:	No

Minaccia 4	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 5	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 6	Accesso abusivo da postazione locale
Data Rilevamento	15/05/2018
Rischio individuato	Visione, Modifica, Copia, Cancellazione abusiva dei dati personali
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Autenticazione Utente, Formazione del personale, Identificazione utente, Procedura blocco postazione
Rischio residuale:	No

Minaccia 7	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato

Rischio residuale:	No

Minaccia 8	Attacchi contro componenti Web
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Indisponibilità dei dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Blocco all'installazione di sw dannosi attraverso "programmi potenzialmente indesiderati", Controllare le impostazioni dell'applicazione e del browser per evitare comportamenti indesiderati in base alle impostazioni predefinite (in particolare per i dispositivi mobili), Evitare l'installazione di plugin del browser a meno che non siano di origine attendibile, Filtrare il traffico web per individuare gli attacchi apportati con tecniche di oscuramento, Monitoraggio del comportamento del software per rilevare componenti dannosi (come i plug-in del browser web), Protezione delle postazioni da software non aggiornato contenente vulnerabilità note
Rischio residuale:	No

Minaccia 9	Accesso abusivo da postazione remota
Data Rilevamento	15/05/2018
Rischio individuato	Copia, visione, modifica, cancellazione dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Attivazione restrizioni software, Formazione del Personale, Installazione e configurazione firewall software
Rischio residuale:	No

Minaccia 10	Denial of Service - Attacchi finalizzati ad impegnare completamente la larghezza di banda di una rete o a sovraccaricare le risorse di un sistema informatico al punto da rendere inutilizzabili per i client i servizi da essi offerti.
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore

Contromisure adottate:	Creazione di policy di sicurezza DoS / DDoS comprensive di un piano di reazione agli incidenti rilevati, Rivalutare regolarmente l'efficacia dei controlli implementati e prevederne lo sviluppo di nuovi, Scelta di un approccio tecnico di protezione DoS / DDoS, Un sistema di prevenzione delle intrusioni (IPS) è la base per identificare altri tentativi di intrusione., Utilizzo di ISP che implementano misure di protezione DDoS
Rischio residuale:	No

Minaccia 11	Intercettazione dei dati durante le operazioni di trattamento (sniffing)
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Utilizzo di protocollo HTTPs. Tutte le trasmissioni utilizzano crittografia ben configurata e potente tramite TLS 1.0 o versioni successive.
Rischio residuale:	No

Minaccia 12	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 13	Malfunzionamento software
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Alterazione dei dati personali
Ambito di interesse della minaccia	Tutte le applicazioni software
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Assistenza software. Backup dei dati su supporto removibile.
Rischio residuale:	No

Minaccia 14	Furto di Hardware
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati, Diffusione dei dati personali
Ambito di interesse della minaccia	

Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Crittografia dei dati, Immagine disco su Disco fisso rimovibile, Potenziamento o installazione sistema di allarme, Procedura controllo periodico sistema di allarme, Procedura gestione delle chiavi
Rischio residuale:	No

Minaccia 15	Danneggiamento tecnologico delle apparecchiature
Data Rilevamento	15/05/2018
Rischio individuato	Perdita dei dati
Ambito di interesse della minaccia	Tutte gli strumenti elettronici
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Minore
Contromisure adottate:	Piano di controllo periodico delle apparecchiature
Rischio residuale:	No

Minaccia 16	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Valutazione d’Impatto sulla Protezione dei Dati

Data Valutazione Impatto:	15/05/2018
Nome Trattamento	T9 - Gestione documenti cartacei dislocati lontano dalla segreteria
Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE “SCIASCIA E BUFALINO”

Descrizione Sistematica del trattamento

Descrizione:		Gestione documenti cartacei dislocati lontano dalla segreteria
Categoria di dati trattati:		Descrizione: Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305. Tipologia: Altri dati particolari Durata: 20 Anni
		Descrizione: Dati personali non particolari Tipologia: Dati personali non particolari (identificativi, contabili, finanziari, etc.) Durata: 20 Anni
Categoria di soggetti interessati:		Dipendenti e Collaboratori, Fornitori, Alunni e loro genitori.
Categoria di destinatari dei dati:		Solo azienda titolare, Altri soggetti legati da un contratto di servizio all'azienda titolare
Finalità del trattamento:		Gestione documenti cartacei dislocati lontano dalla segreteria. I documenti vengono prelevati dai locali di archivio per essere portati al personale di Segreteria per le necessarie lavorazioni e sviluppo pratiche.
Risorse interessate:	Hardware	
	Software	
	Persone	Unità Organizzativa "Intera Segreteria Scolastica", DIRIGENTE SCOLASTICO PRO-TEMPORE,Unità Organizzativa "Collaboratori Scolastici"
Codice di condotta		

Valutazione necessità e proporzionalità

Base giuridica del trattamento:	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento
Legittimi interessi:	
Diritti degli interessati:	Informazione, Accesso ai dati, Rettifica dei dati, Cancellazione dei dati, Limitazione del trattamento, Portabilità dei dati, Proporre reclamo ad autorità di controllo, Revoca del consenso (L'eventuale revoca del consenso non pregiudica la liceità del trattamento basato sul consenso prestato prima della revoca)
Garanzie su Trasferimenti di dati verso paesi terzi:	Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea
Misure tecniche di sicurezza	I dati vengono trattati in sicurezza ed in particolare e' garantita la riservatezza e l'integrità dei dati e la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.
Misure di sicurezza organizzative	L'accesso ai dati e' consentito solo a soggetti autorizzati.

Rischi per i diritti e le libertà degli interessati

Minaccia 1	Mancata distruzione dei supporti contenenti dati sensibili raggiunta la finalità
Data Rilevamento	15/05/2018
Rischio individuato	Detenzione abusiva di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Formazione personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 2	Allagamento dei locali in cui sono custoditi i dati
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Copia di backup dei dati, Il locale, dove sono presenti i dati, non è dislocato al piano terra/seminterrato/scantinato
Rischio residuale:	No

Minaccia 3	Una prolungata assenza di un incaricato dal posto di lavoro può generare l'impossibilità di accedere a dati personali di un interessato tanto da ledere i suoi diritti
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Processo automatizzato
Rischio residuale:	No

Minaccia 4	Accesso ai locali da parte di soggetti non autorizzati
Data Rilevamento	15/05/2018
Rischio individuato	Accesso illegittimo ai dati, Modifiche indesiderate ai dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Bassa
Gravità dell'evento:	Significativo
Calcolo del rischio:	Minore
Contromisure adottate:	Chiusura Locali e armadi con serrature, Vigilanza dei locali a cura degli incaricati responsabili degli accessi
Rischio residuale:	No

Minaccia 5	Emissione/Accettazione non controllata dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione e/o detenzione non controllata di dati sensibili
Ambito di interesse della minaccia	
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Registro Scarico/Carico documenti sensibili
Rischio residuale:	No

Minaccia 6	Mancata chiusura dei contenitori/armadi dei documenti con dati sensibili
Data Rilevamento	15/05/2018
Rischio individuato	Diffusione non controllata di dati sensibili
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Alta
Gravità dell'evento:	Dannoso
Calcolo del rischio:	Significativo
Contromisure adottate:	Formazione del personale, Verifiche periodiche
Rischio residuale:	No

Minaccia 7	Incendio
Data Rilevamento	15/05/2018
Rischio individuato	Indisponibilità dei dati
Ambito di interesse della minaccia	Tutti gli ambienti
Probabilità dell'evento:	Medio-Bassa
Gravità dell'evento:	Serio
Calcolo del rischio:	Significativo
Contromisure adottate:	Copia di backup dei dati, Installazione di estintori
Rischio residuale:	No

Coinvolgimento delle parti interessate

Responsabile della Protezione Dati	Il titolare del trattamento, dopo essersi consultato con il DPO, ing. Natale Salvatore Barraco, concorda di eseguire una valutazione DPIA di cui al paragrafo (1) dell'art. 35 del GDPR anche se non necessaria per la tipologia di Trattamento.
Opinioni degli interessati o dei loro rappresentanti	Non è stato ritenuto necessario raccogliere le opinioni degli interessati o dei loro rappresentanti

Conclusioni

Il titolare del trattamento dei dati ha concluso che, considerate le mitigazioni in atto, non vi sono rischi residui elevati e che pertanto non è necessario consultare l'autorità di vigilanza.

ANALISI DEI TRATTAMENTI DI DATI PERSONALI

(aggiornato al 25.05.2018)

eseguiti in forma cartacea e/o elettronica e/o telematica e delle modalità di raccolta, di trattamento, di conservazione, di comunicazione e/o diffusione.

Categorie omogenee dei dati:

COD.	TRATTAMENTO	INCARICATI AL TRATTAMENTO
T1	**Alunni/Genitori**	**Dati personali trattati da Docenti, D.S.G.A, D.S.**
T2	**Alunni/Genitori**	**Dati personali trattati da A.T.A., D.S.G.A, D.S.**
T3	**Personale dipendente**	**Dati personali trattati da A.T.A., D.S.G.A, D.S.**
T4	**Collaborazioni professionali**	**Dati personali trattati da A.T.A., D.S.G.A, D.S.**
T5	**Acquisti e fornitori**	**Dati personali trattati da A.T.A., D.S.G.A, D.S.**
T6	**Gestione finanziaria e del bilancio**	**Dati personali trattati da A.T.A., D.S.G.A, D.S.**
T7	**Gestione Istituzionale e Protocollo**	**Dati personali trattati da A.T.A., D.S.G.A, D.S.**
T8	**Archivio Delibere C.d.I., G.E., archivio verbali C.d.C. e C.d.D.**	**Dati personali trattati da persone, anche esterne alla scuola, facenti parte degli organi collegiali**
T9	**Gestione documenti cartacei dislocati lontano dalla segreteria**	**Dati personali trattati da Collaboratori Scolastici e Personale Ausiliario**

Codifica dei tipi di dati Trattati:		**Altre codifiche:**	
P	Dati Particolari	**A.T.A.**	Amministrativo, Tecnico, Ausiliario
PG	Dati Particolari e Giudiziari	**D.S.G.A.**	Direttore dei Servizi Generali e Amministrativi
N	Dati NON (Particolari e/o Giudiziari)	**D.S.**	Dirigente Scolastico

SOGGETTI DEI TRATTAMENTI SOPRAINDICATI

Titolare del trattamento:	ISTITUTO ISTRUZIONE SUPERIORE "SCIASCIA E BUFALINO", C.F.: 93066580817, con sede in VIA CESARO', 36 - 91016 ERICE (TP) – Italia, Rappresentato dal Dirigente Scolastico Pro-tempore
Responsabili esterni del Trattamento	elenco completo e aggiornato dei responsabili del trattamento è disponibile presso la segreteria scolastica all'indirizzo della sede del Titolare del Trattamento ed allegato al presente documento
Responsabile della protezione dei dati (DPO)	ing. Natale Salvatore Barraco – Cell: 3289485541 - natale@barraco.it

PREMESSE GENERALI

per la natura dell'Istituzione Scolastica, il trattamento dei dati sopraindicati può avvenire sia in modalità elettronica che cartacea che telematica sia su archivi locali (all'interno della Segreteria Scolastica) che su Cloud. I dati potranno essere del tipo Comuni/Neutri, Particolari/Sensibili e/o Giudiziari.

Categorie di dati art. 9 e 10 RGPD	Durata del trattamento
Come da Autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 N. 305. Ed ancora dati particolari biometrici con specifico consenso.	I dati personali verranno conservati per il periodo necessario al perseguimento delle finalità istituzionali del trattamento. In particolare, i dati personali saranno trattati per un periodo di tempo pari al minimo necessario e fatto salvo un ulteriore periodo di conservazione che potrà essere imposto da norme di legge. In ogni caso si fa riferimento ai tempi previsti dalle Linee Guida per gli Archivi delle Istituzioni Scolastiche (Allegati alla Circolare del Ministero per i beni e le attività culturali n. 44 del 19/12/2005)

Misure di sicurezza	
Misure di sicurezza tecniche	Per trattamenti effettuati in adempimento di un obbligo legale, l'Autorità Garante ritiene che potranno restare in vigore le misure di sicurezza di cui all'allegato B integrate dalle Misure Minime di Sicurezza di Cui alla Circ. AGID N. 2 Aprile 2017.
Misure di sicurezza organizzative	L'incaricato del trattamento presenta garanzie sufficienti in termini di conoscenza specialistica, affidabilità e risorse, per mettere in atto le misure tecniche e organizzative che assicurano la sicurezza del trattamento. Gli stessi dovranno essere periodicamente formati in particolare sulle nuove tecnologie di trattamento dati.

Documenti in ingresso

- **Documenti Cartacei**

  - Ogni documento cartaceo in ingresso ricevuto tramite posta o ricevuto in busta chiusa consegnata a mano viene di norma consegnato al Dirigente Scolastico, che lo apre, lo esamina e, nei casi di documenti con dati particolarmente riservati o particolari, lo protocolla personalmente nel Registro di Protocollo Riservato e lo custodisce in un Armadio di Protezione**,** chiuso a chiave, ad accesso esclusivo, dentro il proprio ufficio normalmente chiuso a chiave quando non presenziato dal Dirigente stesso. Naturalmente per trattare la pratica relativa il Dirigente può portare il documento a conoscenza di un incaricato, raccomandandogli la massima riservatezza nella gestione del documento stesso e di nuovi documenti prodotti per sviluppare la pratica stessa.

  - I documenti cartacei consegnati aperti alla segreteria vengono comunque consegnati al Dirigente, che opera a quel punto la stessa funzione di filtro evidenziata nel punto precedente. Fanno eccezione i documenti con dati neutri (ad esempio: ricevute di tasse scolastiche o domande di certificazione o di routine), che vengono trattati direttamente dalla Segreteria.

  - I documenti cartacei ricevuti tramite fax pervengono sull'apparecchio sito nella stanza presenziata da Incaricati, e subito consegnati di norma al Dirigente Scolastico. Si dovrà porre attenzione in futuro che venga sempre garantita l'impossibilità che dipendenti non incaricati o estranei ne possano in qualunque modo prendere visione. Peraltro è rarissimo che tramite telefax pervengano documenti contenenti dati di qualche particolarità.

- **Documenti Elettronici**

  - I documenti ricevuti tramite posta elettronica sono scaricati da un incaricato, stampati *in <u>una sola copia</u>* e consegnati subito al Dirigente Scolastico, che ne decide l'iter. È assai raro che contengano dati personali di qualche particolarità.

  - Se la Segreteria Scolastica utilizza software Documentale per la Dematerializzazione con annesso software di Protocollazione Web e Software centralizzato di Gestione della Posta Elettronica, allora la Posta elettronica sarà letta dal Dirigente scolastico o un suo delegato (nominato alla funzione con atto separato) il quale opererà in conformità al “Manuale dl Protocollo” cancellando la posta indesiderata e assegnando la posta utile agli assistenti di Segreteria per lo sviluppo successivo della pratica con le relative indicazioni (Acquisizione documento, Protocollazione, e varie). Potrebbero contenere, anche se al momento si ritiene un evento raro, dati personali di qualche particolarità.

Documenti nella fase di sviluppo della pratica

- La fase principale di sviluppo avviene sia su documento cartaceo che tramite documento informatico.
- I documenti cartacei contenenti dati particolari e/o giudiziari vengono trattati in ambiente ad accesso limitato.
- I documenti informatici contenenti dati particolari e/o giudiziari, saranno trattati all’interno di archivi con protezione di password (sia che si utilizzino semplicemente i PC

e/o il Server di Istituto come contenitore dei dati, sia che si usi una piattaforma documentale Cloud per la memorizzazione dei documenti informatici)

Documenti in uscita

- **I documenti cartacei in uscita** sono mandati all'Incaricato che esegue la protocollazione, a meno che il Dirigente Scolastico non decida che, per la natura del loro contenuto, debbano essere sottoposti a Protocollazione Riservata, che viene eseguita dal Dirigente stesso o da suo delegato (nominato alla funzione con atto separato). In questo ultimo caso, il Dirigente o il Delegato si occupa di fare anche una fotocopia e di archiviare il documento nell'Armadio di protezione dati nella stanza del Dirigente.
  - I documenti, dopo la protocollazione, vengono di regola fotocopiati (per la copia che resta all'Istituto), se non già eseguiti in doppia copia. Se ne occupa un Incaricato (Collaboratore Scolastico) e imbustati da un Incaricato (di norma un Assistente Amministrativo). Poi un Collaboratore Scolastico, incaricato del trattamento, si occupa della spedizione. Dovrà essere posta particolare attenzione che nella fase di eventuale fotocopiatura, comunque eseguita sempre da un Incaricato, se svolta in una stanza ad acceso indiscriminato, non ci siano estranei nelle vicinanze in grado di vedere il documento e che il documento non sia mai lasciato incustodito.
  - I documenti da spedire via fax vengono spediti da un Incaricato avendo cura di anteporre ai fogli da inviare, un frontespizio con i dati della scuola e l'oggetto della documentazione che si sta inviando.
  - Infine la copia rimasta alla Scuola viene archiviata nel fascicolo personale dell'interessato, se riguarda una persona, oppure, se necessario, in uno dei fascicoli intitolati ai vari argomenti, secondo la classificazione sistematica che fa riferimento alle sigle di protocollo.

- **I documenti elettronici in uscita**, vengono spediti per Posta Elettronica da un Incaricato il quale provvederà preliminarmente alla acquisizione del Documento stesso, alla sua protocollazione e classificazione, alla archiviazione ed alla fascicolazione. Qualcuna della fasi descritte precedentemente, possono non essere richieste dal Dirigente Scolastico e/o possono non essere necessarie in relazione alla tipologia di documento trattato.

Documenti PUBBLICATI in Albo on Line e/o Amministrazione Trasparente.

- Sulla base della normativa vigente, l'Istituto Scolastico dovrà pubblicare alcune tipologie di atto in Albo on Line e/o Amministrazione Trasparente.
- Gli atti da pubblicare possono essere preventivamente firmati e/o protocollati sulla base delle indicazioni del Dirigente Scolastico.
- Bisognerà porre particolare attenzione alla pubblicazione di documentazione in cui risultino dati personali se la norma non lo specifica espressamente.
- La pubblicazione dei dati delle assenze, delle situazioni contabili, dei cedolini di stipendio, di contratti, possono ricondurre a dati personali dei dipendenti; pertanto se devono essere pubblicati devono essere dati aggregati (riferentesi ad un insieme di persone appartenenti ad una certa categoria), a meno che una norma o di legge non specifichi diversamente.

FINALITA' DEI TRATTAMENTI

T1 – Alunni	**Dati personali trattati da docenti, D.S.G.A., dal D.S.** **Trattamento dati alunni per la didattica e le altre attività correlate** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE: SE RICHIESTI DA ORGANISMI ISTITUZIONALI, UTILIZZO DEL REGISTRO ELETTRONICO) **Trattamento dati alunni per le attività integrative e complementari** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE: SE RICHIESTI DA ORGANISMI ISTITUZIONALI, UTILIZZO DEL REGISTRO ELETTRONICO)
T2 - Alunni	**Dati personali trattati dal personale A.T.A., D.S.G.A., dal D.S.** **Trattamento dati alunni e loro famiglie per l'attività amministrativa e le altre attività correlate** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI E GIUDIZIARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE: SE RICHIESTI DA ORGANISMI ISTITUZIONALI, UTILIZZO DEL REGISTRO ELETTRONICO) **Trattamento dati alunni per le attività di supporto alla didattica** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE: SE RICHIESTI DA ORGANISMI ISTITUZIONALI, UTILIZZO DEL REGISTRO ELETTRONICO) **Trattamento dati alunni e loro famiglie per le attività integrative e complementari** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE: SE RICHIESTI DA ORGANISMI ISTITUZIONALI, UTILIZZO DEL REGISTRO ELETTRONICO) **Trattamento dati alunni per le attività generali riguardanti la didattica, l'organizzazione e il funzionamento della scuola** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE: SE RICHIESTI DA ORGANISMI ISTITUZIONALI, UTILIZZO DEL REGISTRO ELETTRONICO) **Trattamento dati alunni a scopo assicurativo e gestione infortuni, compresa eventuale applicazione D.Lgs 81/2008** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE: SE RICHIESTI DA ORGANISMI ISTITUZIONALI)
T3 - Personale dipendente	**Dati personali trattati dal personale A.T.A., D.S.G.A., dal D.S.** **Trattamento dati dipendenti e loro famiglie per l'attività amministrativa e le altre attività correlate, anche disciplinari** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI E GIUDIZIARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE SE RICHIESTI DA ORGANISMI ISTITUZIONALI: ANCHE DATI PARTICOLARI e/o DATI GIUDIZIARI) **Trattamento dati dipendenti e loro famiglie in ordine alla retribuzione, previdenza** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALI RICHIESTI DA ORGANISMI ISTITUZIONALI : ANCHE DATI PARTICOLARI) **Trattamento dati dipendenti per le attività generali riguardanti la didattica, l'organizzazione e il funzionamento della scuola** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALI SE RICHIESTI DA ORGANISMI ISTITUZIONALI: ANCHE DATI POTENZIALMENTE PARTICOLARI.) **Trattamento dati dipendenti a finalità di assicurazione, gestione infortuni e malattie professionali, di inabilità al lavoro e simili, del D.Lgs 81/2008** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI DI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALI: ANCHE DATI PARTICOLARI)

T4 - Collaborazioni professionali	**Dati personali trattati dal personale A.T.A., D.S.G.A., dal D.S.** **Trattamento dati dei collaboratori esterni per l'attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri argomenti connessi alla categoria** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALE SOLO DATI COMUNI
T5 – Fornitori Beni e servizi: acquisti, affitti, vendite	**Dati personali trattati dal personale A.T.A., D.S.G.A., dal D.S.** **Trattamento dati amministrativi, fiscali e tutti gli altri argomenti connessi alla categoria** (POTENZIALMENTE O DI FATTO SOLO DATI COMUNI, TRANNE CASI ECCEZIONALI E IMPROBABILI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALE SOLO DATI COMUNI)
T6 - Gestione finanziaria e del bilancio	**Dati personali trattati dal personale A.T.A., D.S.G.A., dal D.S.** **Trattamento dati connessi alla gestione del bilancio e tutti gli argomenti connessi, compresi i rapporti con le banche** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI CONNESSI ALLE RETRIBUZIONI ; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALE ANCHE DATI PARTICOLARI, NON DATI GIUDIZIARI)
T7 - Gestione Istituzionale/ Protocollo/Posta	**Dati personali trattati dal personale A.T.A., D.S.G.A., dal D.S.** **Trattamento protocollazione e archiviazione cartacea dati in ingresso e uscita su tutti gli argomenti** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI E GIUDIZIARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALE ANCHE DATI PARTICOLARI E GIUDIZIARI) **Trattamento protocollazione riservata e archiviazione cartacea riservata di dati in ingresso e uscita su tutti gli argomenti** **Trattamento affari generali** (POTENZIALMENTE 0 DI FATTO ANCHE DATI PARTICOLARI E GIUDIZIARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALI: ANCHE DATI PARTICOLARI E GIUDIZIARI)
T8 - Trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali	**Trattamento di tutti i dati della categoria** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI E GIUDIZIARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALI: SOLO DATI COMUNI)
T9 - Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario	**Dati personali trattati dal personale A.T.A., D.S.G.A., dal D.S.** **Trattamento di tutti i dati della categoria in fase di ricezione, trasporto, consegna e spedizione** (POTENZIALMENTE O DI FATTO ANCHE DATI PARTICOLARI E GIUDIZIARI; NON UTILIZZO ANCHE DEL COMPUTER ; COMUNICAZIONI (POTENZIALMENTE 0 DI FATTO ANCHE DATI PARTICOLARI E GIUDIZIARI; UTILIZZO ANCHE DEL COMPUTER CON SOFTWARE GESTIONALE E CON PROGRAMMI ELABORAZIONE TESTI; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALI: ANCHE DATI PARTICOLARI E GIUDIZIARI) **Trattamento di tutti i restanti dati connessi alla gestione organizzativa e di custodia, alla gestione degli archivi cartacei e al supporto a tutte le altre funzioni** (POTENZIALMENTE ODI FATTO ANCHE DATI PARTICOLARI; NON UTILIZZO ANCHE DEL COMPUTER ; COMUNICAZIONI TELEMATICHE ANCHE POTENZIALI: NESSUNA)

Sigla	Tipo trattamento	C			E			T		
		P	PG	N	P	PG	N	P	PG	N
T1 - Alunni - Dati personali trattati da Docenti e dal Dirigente Scolastico										
T1	didattica e le altre attività correlate	X			X			X		X
T1	attività integrative e complementari	X			X			X		X
T2 - Alunni - Dati personali trattati da A.T.A. D.G.S.A. e dal Dirigente Scolastico										
T2	attività amministrativa e altre attività correlate		X			X		X		X
T2	attività di supporto alla didattica	X			X			X		X
T2	attività integrative e complementari	X			X					X
T2	attività generali riguardanti la didattica, l'organizzazione e il funzionamento della scuola		X			X				X
T2	scopo assicurativo e gestione infortuni, compresa eventuale applicazione D.Lgs 81/2008	X			X			X		
T3 - Personale dipendente - Dati personali trattati da A.T.A. D.G.S.A. e dal Dirigente Scolastico										
T3	attività amministrativa e altre attività correlate, anche disciplinari		X			X		X	X	
T3	Attività relative alla retribuzione, previdenza	X			X			X		
T3	attività generali riguardanti la didattica, l'organizzazione e il funzionamento della scuola	X			X			X		
T3	finalità di assicurazione, gestione infortuni e malattie professionali, di inabilità al lavoro e simili, del D.Lgs 626/94	X			X			X		
T4 - Collaborazioni professionali - Dati personali trattati da A.T.A. D.G.S.A. e dal Dirigente Scolastico										
T4	attività amministrativa, retributiva, previdenziale, fiscale e tutti gli altri argomenti connessi alla categoria	X			X			X		
T5 - Beni/servizi: acquisti/affitti/vendite - Dati personali trattati da A.T.A. D.G.S.A. e dal Dirigente Scolastico										
T5	attività amministrative, fiscali e tutti gli altri argomenti connessi alla categoria			X			X			X
T6 - Gestione finanziaria e del bilancio - Dati personali trattati da A.T.A. D.G.S.A. e dal Dirigente Scolastico										
T6	Attività connesse alla gestione del bilancio compresi i rapporti con le banche	X			X			X		
T7 - Gestione Istituzionale/Protocollo/Posta - Dati personali trattati da A.T.A. D.G.S.A. e dal Dirigente Scolastico										
T7	Trattamento protocollazione e archiviazione cartacea dati in ingresso e uscita su tutti gli argomenti		X			X			X	
T7	Trattamento protocollazione riservata e archiviazione cartacea riservata di dati in ingresso e uscita su tutti gli argomenti		X			X			X	
T7	Trattamento affari generali		X			X			X	
T8 - Trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali										
T8	Trattamento di tutti i dati della categoria		X			X				X
T9 - Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario										
T9	Trattamento di tutti i dati della categoria in fase di ricezione, trasporto, consegna e spedizione		X							
T9	Trattamento di tutti i restanti dati connessi alla gestione organizzativa e di custodia, alla gestione degli archivi cartacei e al supporto a tutte le altre funzioni	X								

T1 - Alunni

Dati personali trattati da docenti, dal D.S.G.A., dal D.S.

INCARICATI DEL TRATTAMENTO:

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intero **corpo insegnante.** Pertanto ogni docente, nel momento in cui è assegnato a far parte del corpo insegnante diventa automaticamente Incaricato di tali Trattamenti e riceve un'apposita nomina scritta con istruzioni specifiche sul trattamento dei dati personali.

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera **segreteria scolastica**. Pertanto ogni Assistente Amministrativo o altro dipendente appositamente nominato dal D.S., nel momento in cui è assegnato a far parte di tale unità organizzativa diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita nomina con istruzioni scritte.

È stata inoltre individuata come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

FINALITA' DEL TRATTAMENTO

1) In generale gestione di dati personali comuni e/o particolari per qualsiasi attività didattica e organizzativa in relazione all'istruzione ed all'assistenza scolastica
2) Attività didattiche e di sorveglianza in relazione alla scelta dell'alunno di avvalersi dell'insegnamento della Religione Cattolica (dato sensibile in quanto idoneo a rivelare con buona probabilità le convinzioni religiose).
3) Registrazione di assenze:
    a. per motivi di salute (Dato particolare in quanto in taluni casi idoneo a rivelare parzialmente lo stato di salute)
    b. familiari (DATO PARTICOLARE) con visione di certificati medici di avvenuta guarigione (DATO PARTICOLARE 0 SENSIBILE IN QUANTO PARZIALMENTE IDONEO A RIVELARE LO STATO DI SALUTE)
4) Giustificazioni di assenze dovute a festività religiose di religioni non cattoliche (dato sensibile in GRADO DI RIVELARE LA CONVINZIONE RELIGIOSA)
5) Presa visione di certificazioni mediche per esonero da educazione fisica con diagnosi (DATO SENSIBILE IN QUANTO IDONEO A RIVELARE LO STATO DI SALUTE)
6) Visione e scrittura per le comunicazioni scuola-famiglia (DATI PARTICOLARI)
7) Gestione di alunni portatori di handicap che incidono sulla didattica e relative documentazione per l'integrazione (DATO PARTICOLARE IN QUANTO IDONEO A RIVELARE LO STATO DI SALUTE)
8) Scrittura di note disciplinari e gestione di registri contenenti tali note e provvedimenti di sospensione, ecc. (DATO PARTICOLARE IN QUANTO LA SUA DIFFUSIONE POTREBBE LEDERE LA DIGNITÀ DELL'INTERESSATO E IL SUO DIRITTO ALLA RISERVATEZZA)
9) Elaborazioni di valutazioni intermedie e finali, nonché votazioni sul profitto, il grado di impegno, la condotta, il profilo psicologico e attitudinale, ecc. di ogni alunno assegnato (DATI PARTICOLARI LA CUI DIFFUSIONE POTREBBE LEDERE LA DIGNITÀ DELL'INTERESSATO E IL SUO DIRITTO ALLA RISERVATEZZA) e scrittura delle stesse su moduli e registri anche elettronici.
10) Gestione di elaborati scritti, in particolare temi di Italiano, riportanti in taluni casi informazioni delicate sulla sfera personale e familiare dell'alunno (DATI PARTICOLARI DI GRADO ELEVATO)
11) Conoscenza ed eventuale utilizzo di informazioni su situazione di problemi di salute dell'alunno che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la

vita dell'alunno come per esempio allergie con pericolo di grave shock anafilattico, asma grave con pericolo di soffocamento, diabete grave, epilessia, cardiopatie gravi, ecc. o imbarazzanti come per esempio disturbi di continenza, ecc. messe a disposizione dai genitori o dall'interessato. Se l'informazione è orale l'insegnante è tenuto al riserbo. Se esiste qualche comunicazione scritta, trattasi di (DATO PARTICOLARE E VA TRATTATO CON PARTICOLARI CAUTELE).

12) Gestione dei registri cartacei di classe (DATI COMUNI E PARTICOLARI). Durante l'orario delle lezioni questi registri sono in classe sulla scrivania, affidati all'insegnante di turno. Al termine delle lezioni vengono raccolti da un Collaboratore Scolastico, incaricato del trattamento, e conservati in luogo sicuro per essere riconsegnati da un Collaboratore Scolastico, incaricato del trattamento, all'inizio delle lezioni.
13) Gestione del registro cartacei del docente (DATI COMUNI E PARTICOLARI). Il docente è responsabile della riservatezza del registro. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del docente che è chiuso a chiave (una chiave di riserva è mantenuta con le dovute cautele dalla scuola).
14) Per quanto concerne il trattamento dei dati in registri elettronici (di classe e personali), il docente in qualità di incaricato è in possesso di una password e di uno username, le quali costituiscono le Sue credenziali di autenticazione. L'utilizzo delle credenziali per la verifica dell'identità degli incaricati consente l'accesso di ciascun utente autorizzato solo alle informazioni strettamente pertinenti al proprio ruolo e relative agli alunni a lui affidati (ulteriori informazioni sono fornite nella nomina).
15) Gestione del registro dei verbali dei Consigli di classe (DATI DI TIPO COMUNE E PARTICOLARE); tale registro è conservato a cura del Dirigente in armadio chiuso a chiave.
16) Gestione registri e documenti in occasione di esami e concorsi.
17) Gestione di elenchi di alunni, dipendenti e genitori per attività varie della scuola come per esempio in caso di visite d'istruzione o viaggi (DATI DI TIPO COMUNE).
18) Partecipazione a commissioni scolastiche che trattano dati personali.
19) Partecipazione alla gestione delle elezioni degli organi collegiali (DATI COMUNI).
20) Partecipazione ad attività di gestione del sindacato interno, con conoscenza di dati anche particolari.
21) Gestione del PTOF (DATI NEUTRI).
22) Gestione dell'orientamento scolastico in ingresso e in uscita (SE COINVOLTI PROFILI PSICOLOGICI IL DATO può essere dato particolare).
23) Nel caso di servizi di mensa, particolari prescrizioni dietetiche che siano idonee a rivelare la religione professata o lo stato di salute (DATI PARTICOLARI). Vale anche per elenchi alunni con particolari diete in occasione di viaggi della scuola o di ospitalità di alunni di altre scuole.

MODALITÀ DI RACCOLTA DEI DATI:

1) Gran parte dei dati provengono dall'interno della scuola stessa o dalla visione di dati presenti nel Fascicolo Personale detenuto dalla scuola o presente sul Cloud scolastico.
2) Alcuni dati provengono dalla visione del libretto personale dello studente o da comunicazioni scritte della famiglia o da comunicazioni verbali dello studente.
3) I certificati medici (in caso di esonero da Educazione Fisica) provengono dalla scuola.
4) I temi sono, ovviamente, raccolti direttamente dall'interessato.

MODALITÀ' DI TRATTAMENTO:

1) I registri sono detenuti dagli interessati oppure conservati in luogo chiuso o affidati ad incaricati di riceverli.
2) Eventuali documenti rilevanti sono consegnati alla segreteria.

3) Certificati medici per esonero da educazione fisica o limitazione dell'attività sono consultati e poi restituiti alla segreteria
4) Certificati medici e altri documenti di natura particolare e non, relativi a particolari interventi didattici (p.es. integrazione di alunni portatori di handicap), sono consultati e poi restituiti alla segreteria.
5) Gli elaborati degli studenti sono di norma custoditi in archivio sicuro. Nei casi contenessero dati particolari, vengono consegnati in busta chiusa alla segreteria per una conservazione in luogo ad accesso limitato.

ARCHIVI CARTACEI UTILIZZATI:

- Archivio corrente alunni (contiene Fascicoli Personali)
- Archivio registri e prospetti
- Archivio degli elaborati dell'anno corrente

ARCHIVI ELETTRONICI UTILIZZATI:

- Server Scolastico, Spazio CLOUD per i software su piattaforma Cloud
- Archivio alunni
- Fascicoli Personali
- Archivio registri e prospetti

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI

- Archivio alunni
- Fascicoli Personali
- Archivio registri e prospetti
- Archivio comunicazioni posta elettronica e varie

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA:

1) Elenchi anagrafici (contenenti dati comuni) ad enti pubblici e a privati in occasione di visite guidate, viaggi e simili.
2) Eventuali comunicazioni obbligatorie da eseguire su richiesta di Organismi Pubblici.

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.

Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI

Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza, pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

T2 - Alunni

Dati personali trattati dal Personale A.T.A, dal D.S.G.A., dal D.S.

INCARICATI DEL TRATTAMENTO:

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera **segreteria scolastica**. Pertanto ogni Assistente Amministrativo o altro dipendente appositamente nominato dal D.S., nel momento in cui è assegnato a far parte di tale unità organizzativa diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita nomina con istruzioni scritte.

È stata inoltre individuata come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

FINALITA' DEL TRATTAMENTO

Atti connessi all'iscrizione

1) Istituzione e gestione di un fascicolo personale che accompagnerà l'alunno in tutta la sua carriera e che conterrà tutti i documenti riferibili a lui individualmente, nonché le pagelle pregresse e l'allegato con la valutazione sull'insegnamento della religione. Contiene anche la foto dell'alunno (tipo "fototessera"). Al termine della carriera scolastica o in caso di ritiro viene conservato in un archivio storico (dati comuni, particolari, anche particolari o giudiziari, in questi casi vengono conservati in un archivio separato ad accesso limitato oppure, se trattasi di dati elettronici dovranno essere criptati e conservati su supporti di memorizzazione ad accesso limitato).
2) Gestione degli atti connessi alla preiscrizione, all'iscrizione iniziale e annuale
3) Gestione documento di scelta da parte dell'alunno di avvalersi dell'insegnamento della Religione Cattolica (DATO PARTICOLARE IN QUANTO IDONEO A RIVELARE CON BUONA PROBABILITÀ LE CONVINZIONI RELIGIOSE); Gestione dell'allegato della pagella con la valutazione dell'eventuale insegnamento della religione (DATO PARTICOLARE IN QUANTO IDONEO A RIVELARE CON BUONA PROBABILITÀ LE CONVINZIONI RELIGIOSE)
4) Gestione delle tasse e contributi scolastici, di richieste e di documentazioni per ottenere esoneri da tasse e contributi o per ottenere benefici economici quali sussidi, borse di studio o libri scolastici (IN TALUNI CASI CI SONO DOCUMENTI CON DATI PARTICOLARI (REDDITI, COPIA DI DICHIARAZIONI IRPEF DA CUI SI EVINCONO REDDITI E PATRIMONIO IMMOBILIARE E ALTRE NOTIZIE PARTICOLARI; COMPOSIZIONE DEL NUCLEO FAMILIARE ANCHE IN SEGUITO A DIVORZIO, STATO DI GENITORE CELIBE/NUBILE, ATTESTAZIONE DI ASSEGNI RICEVUTI DAL CONIUGE DIVORZIATO o SEPARATO; in alcuni casi ci sono dati giudiziari e dati particolari)
5) Gestione di elenchi di alunni, dipendenti e genitori per attività varie della scuola
6) Gestione degli elenchi degli alunni e genitori per l'elezione Organi Collegiali
7) Gestione di documenti riferiti a stranieri immigrati, con la possibilità che i dati siano idonei a rivelare l'origine etnica o razziale o la religione (DATI PARTICOLARI)
8) Eventuali documenti riferiti a vaccinazioni obbligatorie (DATO PARTICOLARE) O all'inosservanza dello stesso (DATO PARTICOLARE, PERCHÉ IDONEO A RIVELARE STATO DI SALUTE 0 CONVINZIONI FILOSOFICHE)
9) Gestione delle certificazioni di altri enti su stati e qualità (iscrizione, frequenza, profitto, esiti

scolastici, carriera scolastica, ecc.)

10) Gestione di documenti che attestano quale è la persona esercente la della responsabilità genitoriale per alunni minorenni in situazione particolare o in stato di affido ecc. (IN TALUNI CASI CI SONO DOCUMENTI CON DATI PARTICOLARI RISERVATISSIMI COME PER ESEMPIO LA COMPOSIZIONE DEL NUCLEO FAMILIARE ANCHE IN SEGUITO A DIVORZIO 0 SEPARAZIONE, SENTENZE DI AFFIDO, ECC. IN CASI RARISSIMI CI DONO DATI GIUDIZIARI E DATI PARTICOLARI)
11) Gestione di certificazioni e altri documenti sulla presenza di handicap che incidono sulla didattica (DATO PARTICOLARE IN QUANTO IDONEO A RIVELARE LO STATO DI SALUTE). Gestione dì copie e risultati di test psicologici o psicoattitudinali (RARISSIMI, MA POSSONO ESSERE DATO PARTICOLARE)
12) Gestione delle certificazioni di altri enti su stati e qualità (iscrizione, frequenza, profitto, carriera scolastica, ecc.)
13) Redazione e trasmissione, anche per via telematica, ad altre scuole di foglio notizie alunni, con informazioni sulla carriera scolastica e i documenti in possesso della scuola (DATI COMUNI, IN QUALCHE CASO PARTICOLARI)

Atti gestione corrente

1) Gestione anagrafica dell'alunno con registrazione del pagamento delle tasse, degli esiti finali dell'anno scolastico, dei nominativi dei genitori o esercenti la patria potestà mediante programma informatico che richiede autenticazione ed identificazione di accesso (TUTTI DATI COMUNI O IN RARI CASI PARTICOLARI)
2) Registrazione di assenze per motivi di salute (DATO PARTICOLARE IN QUANTO IN TALUNI CASI IDONEO A RIVELARE PARZIALMENTE LO STATO DI SALUTE) o familiari (DATO PARTICOLARE) con visione di certificati medici di avvenuta guarigione (DATO PARTICOLARE IN QUANTO PARZIALMENTE IDONEO A RIVELARE LO STATO DI SALUTE); giustificazioni di assenze dovute a festività religiose di religioni non cattoliche (DATO PARTICOLARE IN GRADO DI RIVELARE LA CONVINZIONE RELIGIOSA).
3) Gestione di certificazioni mediche per esonero da educazione fisica (DATO PARTICOLARE IN QUANTO IDONEO A RIVELARE LO STATO DI SALUTE)
4) Gestione di note disciplinari e provvedimenti disciplinari gravi quali sospensione, espulsione, ecc. (DATO PARTICOLARE IN QUANTO LA SUA DIFFUSIONE POTREBBE LEDERE LA DIGNITÀ DELL'INTERESSATO E IL SUO DIRITTO ALLA RISERVATEZZA)
5) Gestione di valutazioni intermedie e finali, nonché votazioni, sul profitto, il grado di impegno, la condotta, il profilo psicologico e attitudinale, ecc.(dati PARTICOLARI LA CUI DIFFUSIONE POTREBBE LEDERE la dignità dell'interessato e il suo diritto alla riservatezza)
6) Gestione di certificazioni mediche a seguito di infortuni a scuola per denuncia a Questura, Inail, assicurazione della scuola (dato particolare in grado di rivelare lo stato di salute).
7) GESTIONE DI PAGELLE, DIPLOMI, PROSPETTI DEGLI ESITI E DELLE AMMISSIONI AGLI ESAMI, REGISTRO DEI VOTI E DELLE ASSENZE, REGISTRO DEGLI ESAMI DI MATURITÀ E DI IDONEITÀ O INTEGRATIVI (DATI PARTICOLARI). LA GESTIONE DEI REGISTRI DEI VOTI E DELLE ASSENZE E DEL REGISTRO DEGLI ESAMI DI MATURITÀ È ESEGUITO IN FORMA CARTACEA E IN FORMA ELETTRONICA MEDIANTE PROGRAMMA INFORMATICO CHE RICHIEDE AUTENTICAZIONE ED IDENTIFICAZIONE DI ACCESSO.
8) Esecuzione di certificazioni della scuola stessa o di altri enti su stati e qualità (iscrizione, frequenza, profitto, carriera scolastica, ecc.)
9) Esecuzione di lettere alla famiglia su profitto, mancanze disciplinari, comportamenti inadeguati, assenze ingiustificate e altro (IN ALCUNI CASI I DATI SONO PARTICOLARI)
10) Gestione di lettere o documenti provenienti dagli alunni o dalla famiglie che segnalino comportamenti inadeguati o censurabili da parte di docenti o del personale o di altri alunni, ivi comprese petizioni e richieste di ispezioni da parte delle Autorità scolastiche superiori (IN

ALCUNI CASI SI TRATTA DI DATI PARTICOLARI, MERITEVOLI DI PROTEZIONE PERCHÉ IDONEI A LEDERE QUANTOMENO LA DIGNITÀ DELLA PERSONA CHE NE È OGGETTO).

11) Documenti o comunicazioni della famiglia su situazione di problemi di salute dell'alunno che possono presentarsi durante le lezioni, in alcuni casi con grave rischio per la vita dell'alunno quali allergie con pericolo di grave shock anafilattico, asma grave con pericolo di soffocamento, diabete grave, epilessia, cardiopatie gravi, ecc. o imbarazzanti come disturbi di continenza, ecc. o che necessitano di assenze parziali per terapie (DATI PARTICOLARI).
12) Consegna di elenchi diplomati alle aziende che lo richiedono, contenente dati comuni e particolari mai con votazione. Gli alunni sono inseriti in questi elenchi solo su richiesta ed esplicito consenso.
13) Gestione dell'orientamento scolastico in ingresso e in uscita (SE COINVOLTI PROFILI PSICOLOGICI IL DATO PUÒ ESSERE PARTICOLARE)
14) Gestione dei prestiti della biblioteca (DATI COMUNI)
15) Nel caso di servizi di mensa, gestione di particolari prescrizioni dietetiche che siano idonee a rivelare la religione professata o lo stato di salute (DATI PARTICOLARI). Vale anche per elenchi alunni con particolari diete in occasione di viaggi della scuola o di ospitalità di alunni di altre scuole.

Attività extrascolastiche o integrative

1) Gestione di pratiche per la partecipazione di alunni a tirocini formativi/stages/Alternanza Scuola Lavoro (DATI COMUNI)
2) Gestione delle pratiche riferite a organizzazione di viaggi con agenzie di viaggio: Verifica dei requisiti di legge e della convenienza economica: (DATI COMUNI E IN QUALCHE CASO PARTICOLARI). Gestione delle pratiche di selezione degli autotrasportatori per trasporto di alunni: Verifica dei requisiti di legge e della convenienza economica (DATI COMUNI E IN QUALCHE CASO PARTICOLARI)
3) Gestione di attività extrascolastiche quali attività sportive o altro: verifica dei requisiti di legge e della convenienza economica (DATI COMUNI E IN QUALCHE CASO PARTICOLARI)

Dati neutri

1) Gestione delle pratiche relative alla determinazione del numero delle classi e del relativo organico (DATI ANONIMI); in alcuni casi la presenza di alunni con handicap implica uno specifico riferimento e la possibilità di risalire in forma indiretta all'interessato (DATO POTENZIALMENTE PARTICOLARE)
2) Gestione di statistiche in genere sugli alunni (DATI ANONIMI) e invio delle stesse ad enti pubblici. Redazione di statistiche per l'analisi della dispersione scolastica e rispetto dell'obbligo scolastico (DATO ANONIMO)
3) Gestione dell'iter per l'adozione dei testi scolastici (DATI COMUNI O NEUTRI)
4) Trattamento della determinazione del Calendario scolastico
5) Gestione del PTOF (DATI NEUTRI)

Atti rari o straordinari

1) Partecipazione alla gestione delle pratiche relative ad eventuali denunce per violazioni penali (DATO GIUDIZIARIO). Trattamento di eventuali atti giudiziari per casi particolari e rarissimi (DATO GIUDIZIARIO DA TRATTARE CON ESTREMA CAUTELA)
2) Partecipazione agli atti relativi all'applicazione dell'obbligo scolastico a casi particolari (DATI

ANCHE PARTICOLARI). Eventuali atti riferiti a interventi dell'autorità per inosservanza dell'obbligo scolastico (DATO PARTICOLARE E IN ALCUNI CASI SENSIBILE)

MODALITÀ DI RACCOLTA DEI DATI:

1) Gran parte dei dati provengono dall'interessato
2) Per chi è trasferito o comunque proviene da altra scuola, quest'ultima trasmette un foglio notizie e la parte rilevante del Fascicolo Personale (documenti anagrafici, documenti scuola dati statistici, eventuale certificato di vaccinazione, eventuali certificati medici)
3) Alcuni dati provengono dalla visione del libretto personale dello studente o da comunicazioni scritte della famiglia o da comunicazioni verbali dello studente

MODALITÀ DI TRATTAMENTO:

1) Una parte della gestione del Fascicolo Personale è realizzata senza l'ausilio di strumenti elettronici. Nel momento in cui l'Istituto scolastico adotta un sistema di Dematerializzazione e Gestione documentale su Cloud, allora il fascicolo elettronico da quel momento in poi sarà trattato con strumenti elettronici e su CLOUD.
2) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi o con apposito software.
3) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno in genere corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati. Con l'utilizzo di piattaforme di dematerializzazione, questa corrispondenza non ci sarà più in quanto i dati saranno depositati nei contenitori Cloud e la copia periodica degli stessi sarà curata dai gestori delle piattaforme documentali.

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Tutti i dati ed i documenti sono memorizzati, di norma, nel disco fisso di un server di rete o sul disco fisso del PC in uso o su una piattaforma Cloud per archiviazione documentale, che fornisce i servizi di autenticazione ed identificazione dell'utente. Nel primo e nel terzo caso i dati sono accessibili da tutte le postazioni della rete della segreteria tramite opportuna identificazione della postazione stessa.

1) Apposito software per Gestione Anagrafica alunni, comprendente carriera scolastica, esiti finali, ecc.
2) Apposito software per Gestione Votazioni analitiche nel corso dell'anno scolastico e finali.
3) Apposito software per la gestione degli esami
4) Documenti redatti con programma di elaborazione testi o di foglio elettronico e normalmente salvati nel disco fisso del server di segreteria. In casi sporadici e del tutto eccezionali possono essere memorizzati nel disco fisso della postazione da cui viene redatto.
5) Backup (copia di sicurezza) dei dati degli archivi elencati nei punti precedenti, realizzato su CD/DVD/NAS che successivamente vengono conservati in armadio blindato ad accesso limitato.
6) Elenchi anagrafici contenenti dati comuni, ad A.S.L. (se richiesti per controlli o per organizzazione di attività mediche a favore degli alunni), altre istanze organizzative dell'organizzazione dell'istruzione pubblica per graduatorie o simili, ad enti pubblici e a privati in occasione di

visite guidate, viaggi e simili. Supporto: documenti cartacei o messaggi di posta elettronica o fax.

7) A Inail e Questura per denuncia infortuni, ed eventualmente anche a Società assicuratrice privata, previo consenso se trattasi di dati particolari. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
8) Statistiche (dati anonimi) a enti locali e ad altre istanze organizzative dell'organizzazione dell'istruzione pubblica. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
9) Corrispondenza con enti pubblici di supporto alla didattica, alla ricerca didattica, ai sistemi di valutazione, ecc. In genere non richiedono dati particolari. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
10) Corrispondenza con organismi pubblici italiani e dell'U.E. e altre scuole straniere per la gestione di progetti speciali. In genere non richiedono dati particolari. Supporto: documenti cartacei **o** messaggi di posta elettronica o fax.
11) Comunicazione dati anonimi per adozione libri di testo, anche a privati. Supporto: documenti cartacei o messaggi di posta elettronica o fax.

ARCHIVI CARTACEI UTILIZZATI:

1) Archivio corrente alunni (contiene Fascicoli Personali)
2) Archivio storico alunni (contiene Fascicoli Personali)
3) Archivio registri e prospetti
4) Archivio Diplomi
5) Archivio di corrispondenza generale (esclusa le corrispondenza con singoli che dispongano di Fascicolo Personale)
6) Archivio degli elaborati dell'anno corrente
7) Archivio storico degli elaborati
8) Archivio delle prove d'esame dell'anno corrente e storico
9) Archivio affari generali alunni corrente
10) Archivio affari generali alunni storico

ARCHIVI ELETTRONICI UTILIZZATI (nel caso in cui la Segreteria Scolastica utilizzi un sistema di dematerializzazione e archiviazione documentale su piattaforma Cloud):

1) Archivio corrente alunni (contiene Fascicoli Personali)
2) Archivio storico alunni (contiene Fascicoli Personali)
3) Archivio registri e prospetti
4) Archivio Diplomi
5) Archivio di corrispondenza generale (esclusa le corrispondenza con singoli che dispongano di Fascicolo Personale)
6) Archivio affari generali alunni corrente
7) Archivio affari generali alunni storico

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA:

1) Per chi è trasferito ad altra scuola pubblica, a quest'ultima viene trasmesso un foglio notizie e la parte rilevante del Fascicolo Personale (documenti anagrafici, documenti scolastici, eventuale certificato di vaccinazione, mentre eventuali certificati medici soltanto su consenso dell'interessato. Supporto: documenti cartacei o files.
2) Ad altra scuoia di grado superiore per prescrizioni. Supporto: documenti cartacei o files.

3) Elenchi anagrafici contenenti dati comuni, ad ASL (se richiesti per controlli o per organizzazione di attività mediche a favore degli alunni), altre istanze organizzative dell'organizzazione dell'istruzione pubblica per graduatorie o simili, ad enti pubblici e a privati in occasione di visite guidate, viaggi e simili. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
4) A Inail e Questura per denuncia infortuni. Supporto: documenti cartacei o files. Eventualmente anche a Società assicuratrice privata, previo consenso se trattasi di dati particolari. Supporto: documenti cartacei o messaggi di posta elettronica o fax
5) Trasmissione ad enti pubblici di particolari pratiche, su richiesta dell'interessato, per ottenere determinati benefici. Supporto: documenti cartacei o files.
6) Statistiche (dati anonimi) a enti locali e ad altre istanze organizzative dell'organizzazione dell'istruzione pubblica. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
7) Corrispondenza con enti pubblici di supporto alla didattica, alla ricerca didattica, ai sistemi di valutazione, ecc. In genere non richiedono dati particolari. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
8) Corrispondenza con organismi pubblici italiani e dell'U.E. e altre scuole straniere per la gestione di progetti speciali. Non richiedono dati particolari. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
9) Comunicazione dati anonimi per adozione libri di testo, anche a privati. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
10) Pubblicazione all'albo di prospetti con esiti scolastici intermedi, finali, di ammissione a esami, di risultato degli esami., nonché di elenchi di ammessi all'Istituto o ad altre iniziative. Supporto: documenti cartacei

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.
Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI
Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza, pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

T3 - Personale dipendente

Dati personali trattati da A.T.A., D.G.S.A. e dal Dirigente Scolastico

INCARICATI DEL TRATTAMENTO:

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera **segreteria scolastica**. Pertanto ogni Assistente Amministrativo o altro dipendente appositamente nominato dal D.S., nel momento in cui è assegnato a far parte di tale unità organizzativa diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita nomina con istruzioni scritte.

È stata inoltre individuata come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

FINALITA' DEL TRATTAMENTO

a) Istituzione e gestione di un fascicolo personale che accompagnerà il dipendente in tutta la sua carriera presso l'Istituto (compreso il periodo di quiescenza) e che conterrà tutti i documenti a lui individualmente riferibili, nonché i documenti ricevuti da altre scuole o enti (DATI ANCHE PARTICOLARI). Al termine della carriera scolastica o in caso di ritiro o in caso di trasferimento, il fascicolo viene conservato in un archivio storico (dati comuni, particolari, anche particolari o giudiziari), in questi casi vengono conservati in un archivio separato ad accesso limitato oppure, se trattasi di dati elettronici dovranno essere criptati e conservati su supporti di memorizzazione ad accesso limitato. Tale fascicolo contiene tutti i documenti personali, tranne quelli particolari o giudiziari o particolari archiviati a parte.
b) Comunicazione ad altre scuole o da altre scuole di assunzione in servizio, di assenze, di particolari concessioni e di altri atti nel caso di docenti utilizzati a scavalco da più scuole; di orario scolastico, di impegni per riunioni, ecc., di partecipazione ad esami ed altre attività (DATI COMUNI 0 PARTICOLARI)
c) Gestione di elenchi di alunni, dipendenti e genitori per attività varie della scuola

Assenze, permessi, congedi, aspettative e simili

a) Registrazione delle presenze del personale non docente, tramite firma su registro cartaceo o per tramite di rilevatori di presenza successivamente trattate tramite apposito programma informatico (DATI POTENZIALMENTE PARTICOLARI).
b) Gestione certificati medici generici per assenze per malattia (DATO PARTICOLARE)
c) Registrazione delle assenze per malattia (DATO PARTICOLARE) e relativi atti concessivi (DATO PARTICOLARE) La gestione avviene tramite apposito software che richiede autenticazione ed identificazione di accesso.
d) Gestione richieste, certificazioni, dichiarazioni e concessioni di permessi per handicap di un familiare (DATO PARTICOLARE) O relativi alla fruizione di permessi, riduzioni d'orario e simili per motivi di salute o per condizione di handicap o invalidità (DATI PARTICOLARI), aspettativa per motivi di salute (DATO PARTICOLARE), assenze retribuite al 100% perché connesse a ricoveri ospedalieri, gravi patologie o dovute a terapie invalidanti certificate (art. 17 CCNL 2003) (DATO PARTICOLARE) e relativi atti concessivi (DATO PARTICOLARE), permessi retribuiti o congedi per gravi e documentati motivi e per particolari patologie dei familiari come definiti dal codice civile e relativi atti

concessivi (DATO PARTICOLARE), permesso per particolari impegni come per esempio partecipazione a processi, visite o terapie mediche, impegni familiari, ecc. (DATO ANCHE PARTICOLARE), permessi per assistenza ai figli connessi alla legge in vigore (DATO PARTICOLARE).

e) Gestione richieste, certificazioni, dichiarazioni e concessioni relativi a stato di gravidanza e al rischio di aborto o interdizione o astensione o riduzione orario per allattamento (DATI PARTICOLARI).
f) Gestione richieste e concessioni relative a part-time (DATO PARTICOLARE)
g) Trasmissione di concessioni per alcuni di questi atti a Enti pubblici di controllo come Ragioneria dello Stato, INPS, INAIL ecc.
h) Gestione di tutte le altre pratiche per permessi, assenze, congedi, aspettative, ecc., eseguita a volte su moduli cartacei o più spesso mediante programma di elaborazione testi. In quest'ultimo caso i documenti elettronici possono contenere dati particolari.

Carriera-Nomine-Graduatorie, ecc.

a) Gestione di tutte le pratiche relative all'organico, ai trasferimenti e alle utilizzazioni
b) Gestione richieste, certificazioni, dichiarazioni e concessioni su particolari situazioni personali o familiari che danno diritto a punteggi o preferenze (DATI A VOLTE PARTICOLARI) o per utilizzo facilitazioni di graduatoria o di punteggio per trasferimento (DATO PARTICOLARE) Gestione del contratto di assunzione (DATI COMUNI)
c) Gestione richieste, certificazioni, dichiarazioni e concessioni per immissione in ruolo, ricostruzione di carriera, ricongiungimenti di periodi assicurativi e riscatto di periodi a fini pensionistici (DATI PARTICOLARI).
d) Gestione valutazioni del periodo di prova, note di merito o demerito, provvedimenti disciplinari (DATI PARTICOLARI).
e) Pratiche di cessazione o dispensa dal servizio per inidoneità fisica (DATO SENSIBILE), per incapacità o persistente insufficiente rendimento (DATO PARTICOLARE), destituzione per motivi disciplinari (DATO PARTICOLARE) o per reati (DATO GIUDIZIARIO), dispensa dal servizio per esito sfavorevole della prova (DATO PARTICOLARE)
f) Pratiche per la tutela dei dipendenti in particolari condizioni psicofisiche (art. 124 DPR 309/90)
g) Pratiche per riconoscimento di invalidità per causa di servizio (DATO PARTICOLARE)
h) Trasmissione per via telematica al MIUR di dati comuni e particolari relativi all'assunzione in servizio
i) Richiesta del part-time
j) Gestione domande, dichiarazioni, certificazioni, curriculum per inserimento in graduatorie di aspiranti a supplenze (dato particolare e sensibile quando è presente un fatto che può dar diritto a punteggi per ragioni di handicap o invalidità fisica), formazione, gestione e diffusione delle graduatorie (dato pubblico), depennamenti (dato comune). Spesso questa gestione implica comunicazioni, anche telematiche, da e ad altre scuole e al Miur.
k) Gestione delle pratiche relative alle domande di supplenza temporanea, all'inserimento in graduatorie (IN QUALCHE CASO PARTICOLARI) e alla consultazione o diffusione di queste (DATI PUBBLICI)
l) Nomina e gestione carriera del Docente di Religione (POSSIBILE DATO PARTICOLARE)
m) Gestione nomine per commissari d'esami, anche mediante via telematica (DATI COMUNI)
n) Domande di quiescenza e relativa pratica (DATO PARTICOLARE)
o) Richieste e certificazioni di gravidanza per mantenimento del posto di persona non di ruolo e relativi atti concessivi (DATO PARTICOLARE)
p) Il Trattamento di certificati di buona condotta (dato particolare), certificati di sana e

robusta costituzione (dato sensibile), dichiarazione sui carichi pendenti nel casellario giudiziario (DATO GIUDIZIARIO)

Rapporti economici-previdenziali-fiscali

a) Gestione incentivi economici su fondo d'istituto in genere
b) Documentazione da trasmettere al CAF per il mod. 730, contenente notizie sul reddito annuo e sul patrimonio (DATI PARTICOLARI) e sul conferimento a chiese e/o organizzazioni religiose e/o associazioni no-profit (DATO PARTICOLARE), ricevuta in busta chiusa per la trasmissione al CAF (anche la conservazione e la trasmissione è trattamento di dati)
c) Lavoratori a tempo determinato: Gestione della retribuzione con documenti cartacei e programma informatico: calcolo stipendio, cedolino stipendio (DATO PARTICOLARE), prospetti di spesa, scheda fiscale interna (DATO PARTICOLARE), modello 101 (DATO PARTICOLARE), inserimento di assenze e scioperi che comportano riduzione di stipendio (DATO PARTICOLARE), ritenute per delega sindacale (DATO PARTICOLARE) e altre ritenute (DATO PARTICOLARE), gestione fiscale, detrazioni e gestione previdenziale (DATO PARTICOLARE). Gestione richieste e attribuzioni delle detrazioni fiscali anche per dipendenti a tempo indeterminato (DATO PARTICOLARE). Il programma informatico richiede autenticazione ed identificazione di accesso.
d) Gestione trattamenti di missione (DATI COMUNI)
e) Gestione richieste, certificazioni, dichiarazioni e concessioni relativamente a benefici di natura economica, Assegno per Nucleo Familiare (art. 2 legge 153/1988) (DATI N QUALCHE CASO PARTICOLARI)
f) Gestione e trasmissione all'INPS per via cartacea del progetto di liquidazione TFR per ogni dipendente a tempo determinato.
g) Gestione domande di prestiti, cessione del quinto ecc., a volte motivate con ragioni personali o familiari (DATI PARTICOLARI).
h) Denuncia infortuni per via cartacea (DATO PARTICOLARE)
i) Gestione eventuali pignoramenti dello stipendio e di ritenute per eventuali danni erariali (DATO PARTICOLARE)
j) Trasmissione mensile per via telematica all'INPS dei DM10 (DATO ANONIMO)
k) Trasmissione al Tesoro per via cartacea o telematica dei compensi accessori a fine del conguaglio fiscale.
l) Trasmissione dati a NOIPA dei compensi a Cedolino Unico e per i Compensi Fuori Sistema.
m) In generale qualsiasi ulteriore pratica connessa alla gestione del dipendente dal punto di vista retributivo, fiscale, previdenziale e amministrativo.

Sindacali

a) Gestione della dichiarazione di iscrizione a un sindacato con delega al versamento mensile dei contributi (DATO PARTICOLARE), gestione diretta delle ritenute sindacali o trasmissione al Tesoro per via cartacea e/o telematica.
b) Gestione delle dichiarazione di adesione a sciopero e registrazione dell'assenza per sciopero (DATO POTENZIALMENTE PARTICOLARE). Gestione dei permessi per assemblea sindacale (DATO POTENZIALMENTE PARTICOLARE).
c) Trasmissioni dati per ritenute per sciopero al Ministero del Tesoro (DATO PARTICOLARE) per via cartacea o telematica
d) Gestione materiali sindacali, circolari, proclamazioni di sciopero, gestione contratto integrativo della scuola, rapporti con RSU e sindacati
e) Gestione richieste, certificazioni, dichiarazioni e concessioni in relazione a permessi e distacchi per attività sindacali (DATO PARTICOLARE)
f) Gestione rapporti con Rappresentante dei Lavoratori per la Sicurezza (LA NOMINA È DATO

PARTICOLARE)

Varie

a) Esecuzione delle certificazioni della scuola stessa su stati e qualità (DATI PARTICOLARI) e gestione delle certificazioni di altri enti su stati e qualità (DATI PARTICOLARI)
b) Redazione dell'orario di insegnamento di tutti i docenti, con comunicazione anche ad altre scuole per i docenti "a scavalco" (DATI COMUNI)
c) Convocazione di riunioni, consigli di classe, collegio docenti, scrutini ecc., con comunicazione anche ad altre scuole per i docenti "a scavalco" (DATI COMUNI)
d) Gestione richiesta e concessione di autorizzazione a svolgere altre attività lavorative per persone in part-time e di svolgimento di attività libero-professionale (DATI PARTICOLARI)
e) Eventuale cartella sanitaria ai sensi del D.Lgs 81/2008 custodita in busta chiusa (DATO PARTICOLARE) ed eventuale giudizio di idoneità o inidoneità al lavoro (DATO PARTICOLARE). Corrispondenza con dipendenti su particolari situazioni personali o professionali (DATI PARTICOLARI).
f) Eventuali controversie di lavoro (DATO PARTICOLARE)
g) Eventuali denunce per violazioni penali (DATO GIUDIZIARIO)
h) Gestione di pratiche di dipendenti che usufruiscano di permessi o aspettative perché ricoprono cariche pubbliche (DATO POTENZIALMENTE PARTICOLARE).
i) Trasmissione per via telematica al MIUR di dati anonimi per statistiche e gestione organico (DATI ANONIMI), ivi compresi dati anonimi sulle statistiche di partecipazione a scioperi
j) Gestione di corsi e convegni o della partecipazione agli stessi e relative autorizzazioni (DATI COMUNI 0 NEUTRI)
k) Gestione degli atti relativi al collegio docenti e alle commissioni di lavoro formate da docenti
l) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento a volte sono realizzate su modulo cartaceo, più spesso con programma di elaborazione testi. In quest'ultimo caso i documenti elettronici contenenti dati particolari, giudiziari o particolari vengono trattati con la procedura di Protezione Dati
m) Gestione di tutte le altre pratiche citate nell'elenco

MODALITÀ DI RACCOLTA DEI DATI:

1) Gran parte dei dati provengono dall'interessato
2) Per chi è trasferito o comunque proviene da altra scuola, quest'ultima trasmette un foglio notizie e la parte rilevante del Fascicolo Personale
3) Alcuni dati provengono dalla consultazione di archivi elettronici del MIUR.

MODALITÀ DI TRATTAMENTO:

a) La gestione del Fascicolo Personale è realizzata in parte senza l'ausilio di strumenti elettronici e con l'utilizzo di Software di gestione documentale, anche in modalità informatica.
b) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi o con apposito software.
c) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno normalmente corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati. Con l'avvento di software di gestione documentale la copia cartacea sarà interamente abolita e la copia sarà affidata a software

backup locale e/o Cloud.

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Tutti i dati ed i documenti sono memorizzati, di norma, nel supporto di memorizzazione (disco fisso) di un server di rete che fornisce i servizi di autenticazione ed identificazione dell'utente forniti pure dal PC in uso. I dati sono potenzialmente accessibili da tutte le postazioni della rete della segreteria tramite opportuna identificazione della postazione stessa.

1) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi.
2) Tali documenti redatti con programma di elaborazione testi sono normalmente salvati nel disco fisso del server di segreteria. In qualche caso possono essere memorizzati nel disco fisso della postazione da cui viene redatto.
3) Apposito software per Gestione Stipendi Dipendenti. I dati sono memorizzati nel disco fisso del server di segreteria
4) Apposito software per Gestione Presenze Giornaliere Dipendenti
5) Apposito software per Gestione Esami maturità (Alunni/Docenti)
6) Apposito software per Gestione assenza dipendenti e relative concessioni.
7) Backup (copia di sicurezza) dei dati degli archivi elencati nei punti precedenti, realizzato su CD/DVD/NAS che successivamente vengono conservati in armadio blindato ad accesso limitato.
8) Comunicazione ad altre scuole o da altre scuole di assunzione in servizio, di assenze, di particolari concessioni e di altri atti nel caso di docenti utilizzati a scavalco da più scuole; di orario scolastico, di impegni per riunioni, ecc., di partecipazione ad esami ed altri attività. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi. Comunicazione ad altra scuola di dati per graduatorie. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi.
9) Elenchi anagrafici contenenti dati comuni, ad altre istanze organizzative dell'organizzazione dell'istruzione pubblica per graduatorie o simili, ad enti pubblici e a privati in occasione di visite guidate, viaggi e simili. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi.
10) Trasmissione a Miur dei dati di adesione a scioperi (in forma statistica anonima): Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi.
11) Statistiche (dati anonimi) ad altre istanze organizzative dell'organizzazione dell'istruzione pubblica. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi.
12) Ad enti pubblici (Ministero del Tesoro, Miur, USP, Uffici scolastici Regionali, ex-INPDAP, INPS, INAIL, Ministero Finanze, Ragioneria dello Stato, etc.) per comunicazione di dati per graduatorie, assunzione e contratto di lavoro, gestione stipendi, andamento in quiescenza e TFR, attività previdenziale, adempimenti fiscali (ivi compreso anagrafica delle retribuzioni). Supporto: documenti cartacei o messaggi di posta elettronica o fax o fax o flussi o utilizzo di comunicazioni tipo emulatore di terminale sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali. La comunicazione di dati particolari avviene anche in base alle autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 n. 305.
13) A Inail e Questura per denuncia infortuni. Supporto: documenti cartacei messaggi di posta elettronica o fax. Eventualmente anche a Società assicuratrice privata, previo consenso se trattasi di dati particolari. Supporto: documenti cartacei o messaggi di posta elettronica o fax o

flussi.

ARCHIVI CARTACEI UTILIZZATI:

1) Archivio corrente docenti (contiene Fascicoli Personali)
2) Archivio storico docenti (contiene Fascicoli Personali)
3) Archivio registri, prospetti e graduatorie
4) Archivio di corrispondenza generale (esclusa le corrispondenza con singoli che dispongano di Fascicolo Personale)
5) Archivio assenze corrente
6) Archivio assenze storico
7) Archivio stipendi, previdenziali, ecc. corrente
8) Archivio stipendi, previdenziali, ecc. storico
9) Affari generali docenti
10) Affari generali docenti storico

ARCHIVI ELETTRONICI UTILIZZATI (nel caso in cui la Segreteria Scolastica utilizzi un sistema di dematerializzazione e archiviazione documentale su piattaforma Cloud):

1) Archivio corrente docenti (contiene Fascicoli Personali)
2) Archivio storico docenti (contiene Fascicoli Personali)
3) Archivio registri, prospetti e graduatorie
4) Archivio di corrispondenza generale (esclusa le corrispondenza con singoli che dispongano di Fascicolo Personale)
5) Archivio assenze corrente
6) Archivio assenze storico
7) Archivio stipendi, previdenziali, ecc. corrente
8) Archivio stipendi, previdenziali, ecc. storico
9) Affari generali docenti
10) Affari generali docenti storico

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA:

1) Per chi è trasferito ad altra scuola pubblica, a quest'ultima viene trasmesso un foglio notizie e la parte rilevante del Fascicolo Personale (documenti anagrafici, documenti scolastici di attualità, mentre eventuali certificati medici e altri dati particolari o giudiziari soltanto su consenso dell'interessato). Supporto: documenti cartacei
2) Comunicazione ad altre scuole o da altre scuole di assunzione in servizio, di assenze, di particolari concessioni e di altri atti nel caso di docenti utilizzati a scavalco da più scuole; di orario scolastico, di impegni per riunioni, ecc., di partecipazione ad esami ed altri attività. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi.
3) Comunicazione ad altra scuola di dati per graduatorie. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi.
4) Elenchi anagrafici contenenti dati comuni, ad altre istanze organizzative dell'organizzazione dell'istruzione pubblica per graduatorie o simili, ad enti pubblici e a privati in occasione di visite guidate, viaggi e simili. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi.
5) Documentazione da trasmettere al CAF per il mod. 730, contenente notizie sul reddito annuo r. e sul patrimonio (DATI PARTICOLARI) e sul conferimento conferimento a chiese e/o or-

ganizzazioni religiose e/o associazioni no-profit (DATO PARTICOLARE): ricevuta in busta chiusa per la trasmissione al CAF. Supporto: documenti cartacei in busta chiusa o messaggi di posta elettronica.

6) Trasmissione a enti pubblici (domande di prestiti, cessione del quinto ecc., a volte motivate con ragioni personali o familiari particolari (DATI PARTICOLARI O PARTICOLARI). Supporto: documenti cartacei o messaggi di posta elettronica.
7) Gestione eventuali pignoramenti dello stipendio e di ritenute per eventuali danni erariali (DATO PARTICOLARE AD ELEVATA PARTICOLARITÀ): Supporto: documenti cartacei o messaggi di posta elettronica.
8) Trasmissione ad enti pubblici di particolari pratiche, su richiesta del dipendente, per ottenere determinati benefici. Supporto: documenti cartacei o messaggi di posta elettronica.
9) Trasmissione al Tesoro per via cartacea dei compensi accessori a fine del conguaglio fiscale, Supporto: documenti cartacei o messaggi di posta elettronica
10) Trasmissione a Miur dei dati di adesione a scioperi (in forma statistica anonima): Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi.
11) Trasmissione al Tesoro delle ritenute sindacali da operare. Supporto: documenti cartacei o messaggi di posta elettronica o flussi o inserimenti in portale SIDI.
12) Statistiche (dati anonimi) ad altre istanze organizzative dell'organizzazione dell'istruzione pubblica. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
14) Ad enti pubblici (Ministero del Tesoro, Miur, USP, Uffici scolastici Regionali, ex-INPDAP, INPS, INAIL, Ministero Finanze, Ragioneria dello Stato) per comunicazione di dati per graduatorie, assunzione e contratto di lavoro, gestione stipendi, andamento in quiescenza e TFR, attività previdenziale, adempimenti fiscali (ivi compreso anagrafica delle retribuzioni). Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali. La comunicazione di dati particolari avviene anche in base alle autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 n. 305.
13) A Inail e Questura per denuncia infortuni. Supporto: documenti cartacei o messaggi di posta elettronica. Eventualmente anche a Società assicuratrice privata, previo consenso se trattasi di dati particolari. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi
14) A enti pubblici nel caso di dipendenti che usufruiscano di permessi o aspettative perché ricoprono cariche pubbliche. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
15) Messa a disposizione per consultazione o diffusione mediante albo delle graduatorie e di una serie di atti, quali partecipazione di docenti a commissioni, ripartizione del fondo incentivante, ecc. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi
16) A Medico Competente in base al D.Lgs 81/2008. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.

Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI

Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza, pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione

non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

T4 - Collaborazioni professionali

Dati personali trattati da A.T.A., D.G.S.A. e dal Dirigente Scolastico

INCARICATI DEL TRATTAMENTO:

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera **segreteria scolastica**. Pertanto ogni Assistente Amministrativo o altro dipendente appositamente nominato dal D.S., nel momento in cui è assegnato a far parte di tale unità organizzativa diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita nomina con istruzioni scritte.

È stata inoltre individuata come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

FINALITA' DEL TRATTAMENTO

a) Gestione di offerte e curriculum: elementi di storia personale, profilo culturale, profilo attitudinale, relazioni (DATI PARTICOLARI)
b) Gestione di corrispondenza operativa (DATI COMUNI O PARTICOLARI).
c) Trasmissione cartacea o telematica alla Scuola Pubblica di provenienza e solo telematica al Dipartimento della Funzione Pubblica dei dati personali di collaboratori esterni relativamente alle prestazioni economiche.
d) Gestione di contabilità e fiscale (DATI COMUNI E PARTICOLARI). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio.

MODALITÀ DI RACCOLTA DEI DATI:

1) I dati provengono dall'interessato o da altre scuole ed Enti

MODALITÀ DI TRATTAMENTO:

1) I dati possono essere raccolti in un apposito Fascicolo, gestito con o senza l'ausilio di strumenti elettronici.
2) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi o con apposito software.
3) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno normalmente corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati. Con l'avvento di software di gestione documentale la copia cartacea sarà interamente abolita e la copia sarà affidata a software backup locale e/o Cloud.

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Tutti i dati ed i documenti sono memorizzati, di norma, nel supporto di memorizzazione (disco fisso)

di un server di rete che fornisce i servizi di autenticazione ed identificazione dell'utente forniti pure dal PC in uso. I dati sono potenzialmente accessibili da tutte le postazioni della rete della segreteria tramite opportuna identificazione della postazione stessa.

1) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi.
2) Gestione di offerte, preventivi, fatture, onorari, note spese, ecc., di corrispondenza operativa (DATI COMUNI 0 PARTICOLARI).
3) Trasmissione cartacea o telematica all'Ente di provenienza e solo telematica al Dipartimento della Funzione Pubblica dei dati personali, retributivi e fiscali di collaboratori esterni relativamente alle prestazioni economiche.
4) Gestione di contabilità e fiscale (DATI COMUNI E PARTICOLARI). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio.
5) Back up (copia di sicurezza) dei dati degli archivi elencati nei punti precedenti, realizzato su Compact Disk conservati in armadio blindato o su N.A.S. conservato in luogo ad accesso limitato o su Cloud.
6) Corrispondenza con gli interessati. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
7) Trasmissione cartacea o telematica al Dipartimento della Funzione Pubblica dei dati personali, retributivi e fiscali di collaboratori esterni relativamente alle prestazioni economiche per anagrafe delle prestazioni. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali. La comunicazione di dati particolari avviene anche in base alle autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 n. 305.

ARCHIVI CARTACEI UTILIZZATI:

1) Archivio corrente collaboratori esterni
2) Archivio storico collaboratori esterni
3) Archivio corrente fornitori
4) Archivio storico fornitori
5) Archivio corrente connesso alla gestione del Bilancio
6) Archivio storico connesso alla gestione del Bilancio

ARCHIVI ELETTRONICI UTILIZZATI (nel caso in cui la Segreteria Scolastica utilizzi un sistema di dematerializzazione e archiviazione documentale su piattaforma Cloud):

1) Archivio corrente collaboratori esterni
2) Archivio storico collaboratori esterni
3) Archivio corrente fornitori
4) Archivio storico fornitori
5) Archivio corrente connesso alla gestione del Bilancio
6) Archivio storico connesso alla gestione del Bilancio

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI il ESTERNI ALLA SCUOLA:

1) Corrispondenza con gli interessati. Supporto: documenti cartacei o messaggi di posta elettronica o fax.

2) Trasmissione cartacea o telematica al Dipartimento della Funzione Pubblica dei dati personali, retributivi e fiscali di collaboratori esterni relativamente alle prestazioni economiche. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali. La comunicazione di dati particolari avviene anche in base alle autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 n. 305.

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.

Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI

Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza, pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

T5 - Beni e servizi: acquisti, affitti, vendite

Dati personali trattati da A.T.A., D.G.S.A. e dal Dirigente Scolastico

INCARICATI DEL TRATTAMENTO:

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera **segreteria scolastica**. Pertanto ogni Assistente Amministrativo o altro dipendente appositamente nominato dal D.S., nel momento in cui è assegnato a far parte di tale unità organizzativa diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita nomina con istruzioni scritte.

È stata inoltre individuata come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

FINALITA' DEL TRATTAMENTO

a) Gestione degli acquisti e delle vendite di beni e servizi, nonché di affitti e prestazioni: offerte e preventivi, referenze, redazione di relazioni e prospetti comparativi delle offerte, ordini di acquisto, fatture, contratti, operazioni di collaudo (DATI PARTICOLARI).
b) Prestazioni, servizi, forniture ad altre scuole, nonché introiti per affitto sale, spazi per macchinette automatiche distributrici, ecc.
c) Corrispondenza operativa, (DATI COMUNI o PARTICOLARI). I documenti prodotti dalla scuola per lo più sono realizzati mediante programma informatico di elaborazione testi.
d) Gestione di contabilità e fiscale (DATI COMUNI E PARTICOLARI). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio.
e) Gestione dell'inventario della scuola e dei beni di proprietà dell'ente locale.
f) Corrispondenza con l'ente locale in ordine alle forniture di sua competenza
g) Gestione della biblioteca

MODALITÀ DI RACCOLTA DEI DATI:

1) I dati provengono dall'interessato o da altre scuole ed Enti

MODALITÀ DI TRATTAMENTO:

1) I dati sono raccolti in un apposito Fascicolo, gestito con o senza l'ausilio di strumenti elettronici.
2) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi o con apposito software.
3) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno normalmente corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati. Con l'avvento di software di gestione documentale la copia cartacea sarà interamente abolita e la copia sarà affidata a software backup locale e/o Cloud.

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Tutti i dati ed i documenti sono memorizzati, di norma, nel supporto di memorizzazione (disco fisso) di un server di rete che fornisce i servizi di autenticazione ed identificazione dell'utente forniti pure dal PC in uso. I dati sono potenzialmente accessibili da tutte le postazioni della rete della segreteria tramite opportuna identificazione della postazione stessa.

1) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi.
2) Gestione di offerte, preventivi, fatture, onorari, note spese, ecc., di corrispondenza operativa (DATI COMUNI o PARTICOLARI). I documenti prodotti dalla scuola per lo più sono realizzati mediante programma informatico di elaborazione testi.
3) Gestione di contabilità e fiscale (DATI COMUNI E PARTICOLARI). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio.
4) Back up (copia di sicurezza) dei dati degli archivi elencati nei punti precedenti, realizzato su Compact Disk conservati in armadio blindato o su N.A.S. conservato in luogo ad accesso limitato o su Cloud.
5) Corrispondenza con gli interessati e con l'ente locale. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti.

ARCHIVI CARTACEI UTILIZZATI:

1) Archivio corrente fornitori
2) Archivio storico fornitori
3) Archivio corrente connesso alla gestione del Bilancio
4) Archivio storico connesso alla gestione del Bilancio

ARCHIVI ELETTRONICI UTILIZZATI (nel caso in cui la Segreteria Scolastica utilizzi un sistema di dematerializzazione e archiviazione documentale su piattaforma Cloud):

1) Archivio corrente fornitori
2) Archivio storico fornitori
3) Archivio corrente connesso alla gestione del Bilancio
4) Archivio storico connesso alla gestione del Bilancio

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA:

1) Corrispondenza con gli interessati. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
2) Trasmissione cartacea o telematica al Dipartimento della Funzione Pubblica dei dati personali, retributivi e fiscali di collaboratori esterni relativamente alle prestazioni economiche. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali. La comunicazione di dati particolari avviene anche in base alle autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 n. 305.

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.

Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI

Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza, pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

T6 - Gestione finanziaria e del bilancio

Dati personali trattati da A.T.A., D.G.S.A. e dal Dirigente Scolastico

INCARICATI DEL TRATTAMENTO:

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera **segreteria scolastica**. Pertanto ogni Assistente Amministrativo o altro dipendente appositamente nominato dal D.S., nel momento in cui è assegnato a far parte di tale unità organizzativa diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita nomina con istruzioni scritte. Alcuni o tutti questi dati vengono trattati anche dai Revisori dei Conti nelle loro visite periodiche.

È stata inoltre individuata come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

FINALITA' DEL TRATTAMENTO

a) Predisposizione del Bilancio Preventivo e del Conto Consuntivo. Loro trasmissione per via telematica al MIUR. Gestione degli atti connessi al bilancio: mandati, ordinativi di pagamento anche informatici, reversali, rapporti con l'Istituto Cassiere (DATI ANONIMI O PARTICOLARI)
b) Gestione atti connessi al funzionamento del Consiglio d'istituto e della Giunta Esecutiva. Predisposizione e gestione delle delibere.
c) Gestione di preventivi per acquisti di beni e servizi, anche tramite l'utilizzazione telematica del Programma di Razionalizzazione della Spesa per Beni e Servizi della P.A.
d) Gestione dell'Individuazione periodica dell'Istituto Cassiere e dei successivi rapporti con lo stesso.
e) Gestione assicurazioni (DATI COMUNI E PARTICOLARI)
f) Gestione versamenti Irpef e fiscali in genere, previdenziali, ecc.
g) Trasmissione al USP dei dati relativi al fabbisogno economico (DATI ANONIMI)
h) Gestione dei rapporti con i revisori dei conti
i) Gestione dell'affitto di sale, ecc. ; gestione di convenzioni per macchinette bevande e merendine, per conferimento pasti, ecc.
j) Corrispondenza operativa, (DATI COMUNI O PARTICOLARI). I documenti prodotti dalla scuola per lo più sono realizzati mediante programma informatico di elaborazione testi.
k) Gestione di contabilità e fiscale (DATI COMUNI E PARTICOLARI). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio.
l) Gestione del l'inventario, compresa biblioteca (DATI NEUTRI)

MODALITÀ DI RACCOLTA DEI DATI:

1) I dati provengono dall'interessato o dal MIUR o da Enti Pubblici.

MODALITÀ DI TRATTAMENTO:

1) I dati sono raccolti in un apposito Fascicolo, gestito senza l'ausilio di strumenti elettronici

oppure tramite Piattaforma di gestione documentale.

2) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate con programma di elaborazione testi o con apposito software.
3) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati. Con l'avvento di software di gestione documentale la copia cartacea sarà interamente abolita e la copia sarà affidata a software backup locale e/o Cloud.

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Tutti i dati ed i documenti sono memorizzati, di norma, nel disco fisso di un server di rete che fornisce i servizi di autenticazione ed identificazione dell'utente. I dati sono accessibili da tutte le postazioni della rete della segreteria tramite opportuna identificazione della postazione stessa.

1) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi.
2) Gestione di offerte, preventivi, fatture, onorari, note spese, ecc., di corrispondenza operativa (DATI COMUNI O PARTICOLARI). I documenti prodotti dalla scuola per lo più sono realizzati mediante programma informatico di elaborazione testi.
3) Gestione di contabilità e fiscale (DATI COMUNI E PARTICOLARI). In parte sono eseguiti con un programma informatico per la gestione della contabilità e del bilancio.
4) Gestione del bilancio: eseguita con un programma informatico per la gestione della contabilità e del bilancio.
5) Back up (copia di sicurezza) dei dati degli archivi elencati nei punti precedenti, realizzato su Compact Disk conservati in armadio blindato o su N.A.S. conservato in luogo ad accesso limitato o su Cloud.
6) Corrispondenza con gli interessati e con l'ente locale. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
7) Comunicazione e ricezione di dati anonimi e neutri al Miur e altri enti pubblici. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali.

ARCHIVI CARTACEI UTILIZZATI:

1) Archivio corrente fornitori
2) Archivio storico fornitori
3) Archivio corrente Stipendi
4) Archivio storico Stipendi
5) Archivio corrente connesso alla gestione del Bilancio
6) Archivio storico connesso alla gestione del Bilancio
7) Registri e atti del Consiglio d'istituto e della Giunta Esecutiva

ARCHIVI ELETTRONICI UTILIZZATI (nel caso in cui la Segreteria Scolastica utilizzi un sistema di dematerializzazione e archiviazione documentale su piattaforma Cloud):

1) Archivio corrente fornitori
2) Archivio storico fornitori
3) Archivio corrente registro Stipendi
4) Archivio storico registro Stipendi
5) Archivio corrente connesso alla gestione del Bilancio
6) Archivio storico connesso alla gestione del Bilancio
7) Registri e atti del Consiglio d'istituto e della Giunta Esecutiva

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA:

1) Corrispondenza con gli interessati. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
2) Trasmissione cartacea o telematica al Dipartimento della Funzione Pubblica dei dati personali, retributivi e fiscali di collaboratori esterni relativamente alle prestazioni economiche. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali. La comunicazione di dati particolari avviene anche in base alle autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 n. 305.

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.
Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI
Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza, pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

T7 - Gestione Istituzionale/Protocollo/Posta

Dati personali trattati da A.T.A., D.G.S.A. e dal Dirigente Scolastico

INCARICATI DEL TRATTAMENTO:

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera **segreteria scolastica**. Pertanto ogni Assistente Amministrativo o altro dipendente appositamente nominato dal D.S., nel momento in cui è assegnato a far parte di tale unità organizzativa diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita nomina con istruzioni scritte.

È stata inoltre individuata come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

FINALITA' DEL TRATTAMENTO

a) Tutti i documenti in ingresso e in uscita vengono protocollati (DATI COMUNI, PARTICOLARI, PARTICOLARI, GIUDIZIARI), tranne quelli trattenuti dal Dirigente Scolastico per il protocollo riservato e l'archiviazione separata. I documenti protocollati o le mail ricevute vengono passati all'Incaricato che deve trattare la pratica, che si occupa anche dell'archiviazione, della fascicolazione o della spedizione. Tuttavia documenti di valenza istituzionale perpetua o pluriennale sono archiviati a parte. I fonogrammi vengono trascritti e trattati come un documento cartaceo ricevuto. La gestione del protocollo è eseguita mediante l'utilizzo di apposito registro elettronico.
b) corrispondenza operativa (DATI COMUNI O PARTICOLARI). I documenti prodotti dalla scuola per lo più sono realizzati mediante programma informatico di elaborazione testi.
c) Gestione di elenchi di alunni, dipendenti e genitori per attività varie della scuola
d) Gestioni elezioni per organi collegiali (DATI COMUNI)
e) Ricezione di circolari e normativa (DATI NEUTRI)
f) Ricezione di messaggi da parte di Autorità di Pubblica Sicurezza per problemi particolari e gestione del relativo trattamento.
g) Gestione messaggi posta elettronica interna
h) Gestione posta elettronica tramite internet
i) Gestione corrispondenza con gli Enti locali. (DATI NORMALMENTE neutri)

MODALITÀ DI RACCOLTA DEI DATI:

1) I dati provengono dall'interessato o da enti esterni o privati

MODALITÀ DI TRATTAMENTO:

1) I dati sono raccolti in un apposito Fascicolo, gestito senza l'ausilio di strumenti elettronici oppure tramite Piattaforma di gestione documentale.
2) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate con programma di elaborazione testi o con apposito software.

3) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati. Con l'avvento di software di gestione documentale la copia cartacea sarà interamente abolita e la copia sarà affidata a software backup locale e/o Cloud.

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Tutti i dati ed i documenti sono memorizzati, di norma, nel disco fisso di un server di rete che fornisce i servizi di autenticazione ed identificazione dell'utente. I dati sono accessibili da tutte le postazioni della rete della segreteria tramite opportuna identificazione della postazione stessa.

1) Tutte le pratiche che richiedono una risposta o la produzione di un certificato o documento sono realizzate raramente su modulo cartaceo prestampato, più spesso con programma di elaborazione testi.
2) Gestione del protocollo.
3) Corrispondenza con gli interessati, con privati ed enti pubblici. Supporto: documenti cartacei o messaggi di posta elettronica o fax o fonogramma trascritto.
4) Comunicazione e ricezione di dati anonimi e neutri al Miur e altri enti pubblici. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali.
5) Backup (copia di sicurezza) dei dati degli archivi elencati nei punti precedenti, realizzato su CD/DVD/NAS che successivamente vengono conservati in armadio blindato ad accesso limitato.

ARCHIVI CARTACEI UTILIZZATI:

1) Archivio corrente generale
2) Archivio storico generale
3) Archivio corrente Riservato
4) Archivio storico Riservato
5) Registri e atti del Consiglio d'istituto e della Giunta Esecutiva

ARCHIVI ELETTRONICI UTILIZZATI (nel caso in cui la Segreteria Scolastica utilizzi un sistema di dematerializzazione e archiviazione documentale su piattaforma Cloud):

1) Archivio corrente generale
2) Archivio storico generale
3) Archivio corrente Riservato
4) Archivio storico Riservato
5) Registri e atti del Consiglio d'istituto e della Giunta Esecutiva

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA:

1) Corrispondenza con gli interessati. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
2) Trasmissione cartacea o telematica al Dipartimento della Funzione Pubblica dei dati personali, retributivi e fiscali di collaboratori esterni relativamente alle prestazioni economiche.

Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali. La comunicazione di dati particolari avviene anche in base alle autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 n. 305.

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.

Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI

Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza, pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

T8 - Gestione di trattamenti da parte di persone, anche esterne alla scuola, facenti parte degli organi collegiali

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera **segreteria scolastica**. Pertanto ogni Assistente Amministrativo o altro dipendente appositamente nominato dal D.S., nel momento in cui è assegnato a far parte di tale unità organizzativa diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita nomina con istruzioni scritte.

È stata inoltre individuata come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

Il Titolare del Trattamento ha inoltre individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'intera categorie delle **"persone facenti parte degli organi collegiali".** Pertanto ogni persona, nel momento in cui è assegnato a far parte di tali organi diventa automaticamente Incaricato di tali trattamenti e riceve un'apposita istruzione scritta.

FINALITA' DEL TRATTAMENTO

a) Il presidente del C.d.l. convoca le riunioni dell'organo e può mandare della corrispondenza alle famiglie e agli alunni
b) Le persone designate a far parte degli organi collegiali vengono a conoscenza di molti dati neutri, ma anche di dati personali a volte anche particolari
c) Utilizzo di elenchi di alunni, dipendenti e genitori per attività varie della scuola
d) Nel caso di formazione di verbali su registri dei verbali di tali organi, essi possono mettere a verbale dichiarazioni anche importanti e delicate
e) Partecipano alla stesura e approvazione e di delibere del C.d.l. e di atti della G.E. e in vari casi le sottoscrivono.
f) I genitori e gli alunni eletti nei Consigli di classe possono partecipare a trattamenti di dati che riguardano anche terzi
g) I genitori e gli alunni in genere possono partecipare ad attività della scuola, partecipando a trattamenti di dati che trascendono la sfera individuale del loro figlio (ad esempio: organizzazione di corsi di recupero, gite scolastiche, ecc.) però lo fanno in forma episodica e quindi ne rispondono a titolo personale, delibere di C.d.l. e G.E.

I MODALITA' DI RACCOLTA DEI DATI:

1) I dati provengono dalla scuola stessa o da altri alunni o genitori

MODALITA' DI TRATTAMENTO:

1) I trattamenti sono verbalizzati in appositi registri o prendono la forma di deliberazioni.
2) Tutte le informazioni gestite con l'ausilio di supporto elettronico hanno corrispondenza in documenti cartacei, per cui, in caso di guasto elettronico, è possibile ricostruirle mediante i documenti archiviati.

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Dati relativi alle delibere dei vari organi collegiali.

ARCHIVI CARTACEI UTILIZZATI:

1) Archivio corrente delibere di Cdl e GE
2) Archivio storico delibere di Cdl e GE
3) Registri dei verbali dei Consigli di classe, dei Cdl e della GE

ARCHIVI ELETTRONICI UTILIZZATI (nel caso in cui la Segreteria Scolastica utilizzi un sistema di dematerializzazione e archiviazione documentale su piattaforma Cloud):

1) Archivio corrente delibere di Cdl e GE
2) Archivio storico delibere di Cdl e GE
3) Registri dei verbali dei Consigli di classe, dei Cdl e della GE

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA:

1) Corrispondenza con gli interessati. Supporto: documenti cartacei o messaggi di posta elettronica o fax.
2) Trasmissione cartacea o telematica al Dipartimento della Funzione Pubblica dei dati personali, retributivi e fiscali di collaboratori esterni relativamente alle prestazioni economiche. Supporto: documenti cartacei o messaggi di posta elettronica o fax o flussi o utilizzo di comunicazioni su portali Web sulla base di programmi gestiti da tali enti e con base dati gestita da tali enti. Le comunicazioni avvengono sulla base di leggi o regolamenti nazionali. La comunicazione di dati particolari avviene anche in base alle autorizzazioni generali del Garante ed al D.M. 7 Dicembre 2006 n. 305.

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.
Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI
Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza, pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

T9 - Trattamenti di dati personali effettuati da Collaboratori Scolastici e Personale Ausiliario

INCARICATI DEL TRATTAMENTO:

Il Titolare del Trattamento ha individuato come **"Unità organizzativa"** incaricata dei trattamenti sotto elencati l'unità **"collaboratori scolastici".** Pertanto ogni collaboratore scolastico, nel momento in cui è assegnato a far parte del personale dell'Istituto scolastico, diventa automaticamente incaricato di attività che consistono nello spostare, custodire, consegnare o archiviare documenti contenenti i dati personali.

FINALITA' DEL TRATTAMENTO

1) Ricevere, trasportare, consegnare, inviare documenti contenenti dati personali, aperti o collocati in busta chiusa, tra cui i registri.
2) Visionare documenti contenenti dati personali allo scopo di dare indicazioni di massima agli utenti
3) Custodire documenti e registri per brevi periodi
4) Gestione di elenchi di alunni, dipendenti e genitori per attività varie della scuola
5) Fotocopiare e faxare documenti contenenti dati personali
6) Collaborare ad operazioni di archiviazione di documenti cartacei
7) Collaborare ad operazioni di scarto ed eliminazione di documenti cartacei
8) In generale, svolgere attività di supporto a tutti i trattamenti svolti nella scuola.

MODALITÀ DI RACCOLTA DEI DATI:

1) I dati provengono dalla scuola stessa o da altri alunni o genitori o da privati o da Uffici Pubblici o da altri uffici, dagli uffici postali e da spedizionieri, da banche, da Enti.

MODALITÀ DI TRATTAMENTO:

1) Le azioni strettamente necessarie per compiere i trattamenti sopraelencati, da svolgere con diligenza e cautela

ELENCO DEI PRINCIPALI DATI TRATTATI CON L'AUSILIO DI STRUMENTI ELETTRONICI E INDICAZIONE DEI RELATIVI ARCHIVI

Nessuno

ARCHIVI CARTACEI UTILIZZATI:

Collaborazione tecnica alla gestione di tutti gli archivi cartacei dislocati lontano dalla segreteria

ELENCO DEI PRINCIPALI DATI COMUNICATI A ENTI PUBBLICI O A PRIVATI ESTERNI ALLA SCUOLA:
Spedizione o consegna di plichi predisposti dalla Segreteria o dal Dirigente Scolastico.

TRASFERIMENTO DEI DATI AL DI FUORI DELL'UNIONE EUROPEA.
Non è previsto il trasferimento dei dati personali a destinatari al di fuori dell'Unione Europea

CONSERVAZIONE DEI DATI
Tutti i dati personali conferiti saranno trattati nel rispetto dei principi di liceità, correttezza,

pertinenza e proporzionalità, solo con le modalità, anche informatiche e telematiche, strettamente necessarie per perseguire le finalità sopra descritte. In ogni caso, i dati personali saranno conservati per un periodo di tempo non superiore a quello strettamente necessario al conseguimento delle finalità indicate. I dati personali dei quali non è necessaria la conservazione o per cui la conservazione non sia prevista dalla vigente normativa, in relazione agli scopi indicati, saranno cancellati o trasformati in forma anonima.

ANALISI DEI RISCHI

1) OGGETTO E FINALITÀ

In questo documento vengono definiti i criteri e le modalità operative adottate dall'Istituto Scolastico per individuare e valutare i rischi e quindi adottare le misure adeguate alla protezione della sicurezza delle aree, dei dati e delle trasmissioni, al fine di ridurre al minimo i rischi stessi.

2) APPLICABILITÀ

Le indicazioni contenute nel presente documento devono essere utilizzate per gestire i rischi connessi alle attività di trattamento dei dati personali, in seno all'Istituto Scolastico, ma anche da parte dei responsabili esterni.

3) RIFERIMENTI NORMATIVI

Norma	Articolo
D.Lgs. n.196/2003	Art. 31
	Art. 33- 34-35-36
	Allegato B Punto 25
	Art. 180 (disposizioni transitorie)
	Allegato B Punti da 19.1. a 19.8
Norma	Articolo
GDPR UE 2016/679	Art. 32 - 36
	Regolamento UE 2016/679
	Direttiva UE 2016/680
	In attesa del **decreto di armonizzazione e adeguamento della normativa nazionale** alla normativa Europea (atteso entro il 21/08/2018).
	Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248)

4) RESPONSABILITÀ

Il Titolare è responsabile dell'analisi e della valutazione dei rischi ai fini dell'adozione delle misure di sicurezza, sia idonee, sia minime. Il Titolare si avvale del Responsabile della Protezione dei Dati (DPO) per la predisposizione della presente modulistica. In particolare il Dirigente scolastico, Titolare del trattamento, deve adottare le misure minime, ai sensi del disciplinare tecnico del D.Lgs. 196/2003 e del nuovo Regolamento Europeo sulla Protezione dei Dati Personali UE 2016/679, e procedere alla predisposizione delle misure idonee ritenute indispensabili nella struttura di afferenza. Spetta al Titolare del trattamento, valutare la congruità tecnico-economica delle misure proposte e quindi disporre l'adozione delle stesse. Il presente documento sulla sicurezza è approvato dal titolare del Trattamento.

5) CRITERI PER L'INDIVIDUAZIONE DEI RISCHI

Occorre innanzitutto premettere che gli articoli da 33 a 36 del Testo Unico in materia di

Trattamento dei dati personali di cui al D.Lgs. 30 giugno 2003 n.196 prevedono l'obbligo di adottare le misure minime di sicurezza.

Occorre premettere le indicazioni fornite con *Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia digitale,* "Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)»."

Il Regolamento europeo non parla invece di misure minime, ma si esprime solamente in termini di adeguatezza: l'art. 32 GDPR recita infatti che "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio". L'Agid con la circolare N. 2/2017 ha indicato una serie di misure Minime, Standard, Avanzate che si possono tenere in considerazione per la protezione dei dati.

Tali misure debbono essere obbligatoriamente adottate in base all'individuazione di due grandi categorie di rischi:

A. Rischi connessi al mancato rispetto degli adempimenti e delle prescrizioni statuite dal Regolamento in materia di trattamento di dati personali;
B. Rischi propri del sistema di gestione dei dati utilizzato dall'Istituto Scolastico.

Tale distinzione si chiarisce se si considera che i rischi del trattamento della prima categoria si riferiscono direttamente ed unicamente all'intera materia inerente la tutela dei dati personali mentre i rischi sottesi alla seconda si riferiscono all'applicazione pratica, effettiva e funzionale delle misure di sicurezza adottate, tra queste comprese quelle relative alla sicurezza informatica.

L'analisi del rischio è stata, pertanto, affrontata secondo quanto sopra riportato e di conseguenza suddivisa in due settori di rischi propri nettamente differenti e separati per tipologia e materia.

- **PRIMO SETTORE DI RISCHIO:**

In questa fase dell'analisi sono stati individuati e valutati tutti i rischi previsti dalla legge, quali, ad es.:

o il rischio di distruzione accidentale dei dati,
o il rischio di perdita dei dati, o il rischio di accesso non autorizzato,
o il rischio di trattamento di dati non conforme alla finalità della raccolta,
o il rischio di trattamento illegittimo e di trattamento non consentito, che sono potenzialmente insiti in ogni istituto scolastico.

A tal proposito si è ritenuto fondamentale arginare il menzionato problema innanzitutto prevedendo un adeguato ed efficiente piano di formazione degli incaricati del trattamento e ciò in quanto è dato riscontrare anche dalle informazioni e dalle notizie di cronaca che la maggior parte delle violazioni della privacy vengono perpetrate direttamente e quasi unicamente dagli incaricati del trattamento.

Infatti proprio tali soggetti sono potenzialmente idonei ad effettuare in astratto comunicazioni o diffusioni illegittime di dati personali o di utilizzare tali dati per fini non conformi alle finalità del trattamento.

Di tale settore di rischio è necessario occuparsi quindi mediante l'approfondita conoscenza della legge sulla Privacy e dell'attuale Regolamento Europeo.

Si è ritenuto, infatti, che solo un'adeguata conoscenza del disposto normativo possa realmente e proficuamente garantirne l'osservanza del medesimo ed in definitiva possa abbattere

effettivamente i rischi connessi a tale primo settore di rischio che, anche in base all'analisi della mancata registrazione di violazioni del trattamento informatico e/o cartaceo, è stato concordemente ritenuto il più rilevante ed in definitiva quello avverso il quale dedicare le maggiori attenzioni.

- **SECONDO SETTORE DI RISCHIO:**

In questa fase, invece, sono stati identificati e valutati i rischi del sistema informatico e tutti quelli che sono propri della sua normale attività.

Da ciò consegue che proprio nella fase di valutazione dei rischi si devono verificare:

A. l'efficacia degli strumenti impiegati al fine di assegnare al rischio un indice di gravità (quali danni sono stati riscontrati o quali ancora possibili) e di frequenza (intesa a verificare, nonostante la misura adottata) e quindi di individuare le circostanze di manifestazione di attacchi informatici al fine di individuarne anche le consequenziali azioni correttive;
B. le misure che sono risultate non adeguate.

Il processo di individuazione ed ulteriore valutazione dei rischi eventualmente manifestatisi deve essere ripetuto con cadenza almeno annuale e, comunque, immediatamente al verificarsi di rischi gravi connessi al trattamento o segnalati dall'installatore esterno delle misure minime di sicurezza.

Le misure minime di sicurezza devono tendere a ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta. L'adeguatezza delle misure deve essere valutata, secondo le linee guida indicate in questo documento, tenendo conto delle conoscenze acquisite in base al progresso tecnico, alla natura dei dati trattati e alle specifiche caratteristiche del trattamento. A tal proposito si è proceduto all'individuazione dei rischi utilizzando degli appositi strumenti di indagine in cui sono riportati i singoli fattori di rischio: questi sono divisi rispettivamente tenendo conto dei rischi relativi alle aree e locali, all'integrità dei dati e alle trasmissioni. Le matrici sono utilizzate come uno strumento elastico: i singoli responsabili possono adattarle in base all'esperienza maturata, all'anamnesi e alle caratteristiche specifiche dei trattamenti. Si potrà procedere all'analisi dei rischi settore per settore. Si è proceduto all'analisi facendo attenzione a non considerare le misure già adottate: l'analisi è stata fatta con un sistema cosiddetto a rischio zero, valutando astrattamente quali possono essere i rischi, a prescindere dalle misure che sono state già adottate. Ciò serve a verificare se quanto fatto è da considerarsi idoneo, oppure necessiti di interventi adeguativi.

6) CRITERI PER LA VALUTAZIONE DEI RISCHI

Una volta individuati i rischi si è proceduto alla valutazione degli stessi, attraverso una indicizzazione delle possibili perdite. In particolare si è tenuto conto di tre indici:

- **Probabilità (P) di accadimento,** che riguarda la frequenza riscontrata o riscontrabile;
- **Gravità (G) delle conseguenze,** nel caso lo stesso evento si verifichi.
- **Rilevabilità (R)** che indica lo stato di previsione dell'evento (quanto è possibile prevedere in anticipo l'evento)

Il Rischio (Indice di gravità di rischio) altro non è che la risultante del prodotto dei tre fattori

(PxGxR)

probabilità, gravità e rilevabilità di un evento.

Secondo i criteri adottati dando a **P** un valore compreso fra 1 e 10, a **G** ugualmente fra 1 e 10 e a **R** un valore fra 10 e 1 si è ottenuto il valore **I** compreso fra 1 e 1000.

Qui di seguito viene riportata la tabella di valutazione dei vari coefficienti:

PROBABILITÀ DI VERIFICARSI DELL'EVENTO (P)		
Valutazione	**Punteggio**	**Valutazione storica**
Remota	= 1	Non sono noti episodi
Bassa	= 2-3	Sono noti rarissimi episodi
Moderata	= 4-6	Noto qualche episodio in cui è stata rilevata la mancanza la mancanza ma non sono stati rilevati danni
Alta	= 7-8	Noto qualche episodio in cui la mancanza rilevata ha fatto seguito a un danno
Molto alta	= 9-10	Si sono verificati danni per la stessa mancanza rilevata in situazioni simili.

GRAVITÀ AL VERIFICARSI DELL'EVENTO (G)		
Valutazione	**Punteggio**	**Descrizione del danno**
Lieve	= 1	Furto o distruzione dei dati
Significativa	= 2-6	Utilizzo illegale o alterazione dei dati
Grave	= 7-8	Perdita di dati causata da un uso non autorizzato
Estremamente Grave	= 9-10	Perdita dei dati a seguito di diffusione illegale

RILEVABILITA' DEL VERIFICARSI DELL'EVENTO (R)		
Valutazione	**Punteggio**	**Valutazione storica**
Alta	= 1	Facilmente rilevabile con buon anticipo
Moderata	= 2-4	Esistono fattori oggettivi che rilevano il verificarsi dell'evento
Piccola	= 5-7	È possibile rilevare il verificarsi dell'evento utilizzando opportuni mezzi e strumenti di indagine
Molto piccola	= 8-9	Il verificarsi dell'evento è individuabile soltanto in circostanze fortuite e in condizioni non riproducibili
Improbabile	= 10	L'evento non è prevedibile

L'avere fatto l'analisi a rischio zero consente di verificare il grado di efficacia delle misure già adottate. Un esempio può essere utile a chiarire: essere dotati di un firewall comporta che non si possa eludere il rischio di attacchi esterni da parte di hacker (circostanza per la quale non può dirsi di essere al sicuro in assoluto). Il sistema di analisi a rischio zero comporterà che il rischio di attacchi è comunque preso in considerazione, a prescindere dalle misure adottate.

Sarà invece in sede di valutazione e di revisione della valutazione che si dovranno verificare:

A. l'efficacia degli strumenti adottati, attraverso l'analisi dei rapporti di non conformità, dei rapporti delle azioni correttive e dei rapporti delle azioni preventive, al fine di assegnare al rischio un indice di gravità (quali danni si sono avuti o quali possano essere possibili) e di frequenza (intesa a verificare, nonostante la misura adottata) quali siano state le circostanze in cui si sono subiti attacchi;
B. le misure che sono risultate non adeguate.

Il processo di individuazione e valutazione dei rischi deve avvenire con cadenza al massimo annuale, ma può essere ripetuto anche nel corso dell'anno.

7) MISURE DI PREVENZIONE E PROTEZIONE

Le azioni necessarie per l'adozione di idonee misure di sicurezza riguardano:

A. **la prevenzione:** attività che permette di impedire gli accadimenti negativi, agendo direttamente sulla diminuzione delle probabilità di manifestazione delle non conformità;
B. **la correzione:** attività che permette di diminuire la gravità degli effetti causati eventualmente dall'accadimento dell'evento di non conformità.

Dopo aver analizzato e valutato i fattori di rischio, relativi alle aree e locali, all'integrità dei dati e alle trasmissioni, sono state individuate le misure di prevenzione e protezione più idonee a ridurre o eliminare il rischio stesso.

L'insieme delle misure preventive e protettive costituisce un programma di fondamentale importanza nell'ambito della politica per la Sicurezza, poiché fornisce una guida operativa, che permette di gestire la Sicurezza con organicità e sistematicità e in modo dinamico. Per definire uno scadenzario degli interventi l'Istituto Scolastico ha adottato un criterio di "N" mesi crescenti in funzione inversa all'indice di gravità (e quindi al valore del numero "**I**").
Vedere esempio seguente:

I = 500 ÷ 1000	intervento immediato e verifica entro 5 giorni
I = 200 ÷ 500	intervento entro 01 mesi e verifica entro 10 giorni
I = 100 ÷ 200	intervento entro 06 mesi e verifica entro 30 giorni
I = 50 ÷ 100	intervento entro 12 mesi e verifica entro 40 giorni
I = 1 ÷ 50	intervento entro 18 mesi e verifica entro 60 giorni

Il programma delle misure di sicurezza adottate o da adottare per ogni categoria di rischi (aree e locali, integrità dei dati e trasmissioni) è sistematicamente aggiornato nell'ottica di un miglioramento continuo del Sistema Sicurezza dell'Istituto Scolastico: esso è sottoposto a riesame ogni anno, salvo diversa indicazione del Titolare del trattamento o per iniziativa dei responsabili, che riscontrino necessità di intervento o non conformità (tecniche o normative).

Obiettivo delle misure programmate è comunque ridurre al minimo valore possibile l'indice di rischio relativo "**I**" a seguito dell'adozione, da parte dei singoli responsabili, delle misure idonee di protezione proposte al Titolare del Trattamento.

Misure Organizzative

01 Analisi dei rischi
02 Redazione linee-guida sicurezza
03 Istruzioni interne
04 Assegnazione incarichi
05 Formazione professionale
06 Classificazione dei dati
07 Misure graduate per classi dati
08 Consultazioni registrate
09 Controlli periodici
10 Verifiche periodiche per finalità
11 Sorveglianza sulla distruzione
12 Altro

Misure Fisiche

01 Vigilanza della sede
02 Ingresso controllato
03 Sistemi di allarme
04 Registrazione accessi
05 Autenticazione accessi
06 Custodia in classificatori o armadi
07 Deposito in cassaforte
08 Custodia in armadi blindati
09 Dispositivi antincendio
10 Continuità elettrica
11 Verifica leggibilità supporti
12 Altro

Misure Logiche

01 Identificazione utente
02 Autenticazione utente
03 Controllo accessi
04 Registrazione accessi
05 Controlli antivirus
06 Sottoscrizione elettronica
07 Cifratura dati trasmessi
08 Cifratura dati memorizzati
09 Annotazione fonti dei dati
10 Annotazione responsabile delle operazioni
11 Rilevazione intercettazioni
12 Monitoraggio continuo sessioni
13 Sospensione automatica sessioni
14 Verifiche automatizzate dati
15 Controllo supporto dati manutenzione
16 Altro

8) PROGRAMMA DELLE MISURE DI PREVENZIONE E PROTEZIONE

Il programma delle misure di protezione necessarie per il trattamento dei rischi analizzati e valutati, in base ad un criterio quantitativo, sono riportate nelle ceck-list utilizzate per la gestione dei rischi, con la definizione dei tempi previsti per l'adozione. Sono state previste anche le modalità per la verifica dell'adozione delle misure programmate e per il monitoraggio della idoneità delle stesse. I membri del Gruppo Privacy , o personale esterno ed indipendente possono essere incaricati, da parte del Titolare del Trattamento, di svolgere verifiche periodiche, anche mediante visite ispettive, finalizzate a controllare il rispetto degli standard di sicurezza dell'Istituto Scolastico.

8.1) Descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati personali.

Il presente paragrafo è stato elaborato in riferimento al punto 19.5 del disciplinare tecnico del D.Lgs. 196/2003 che impone "la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

Il successivo punto 23 richiamato stabilisce inoltre che "sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni".

La misura di cui sopra è stata chiaramente richiamata nella Circolare N. 2/2017 dell'Agenzia per l'Italia Digitale.

Considerato che ogni sistema informatico deve prevedere un piano di emergenza per soddisfare le specifiche del disciplinare tecnico è necessario, pertanto, riferirsi alle procedure già applicate ed in particolare alla dichiarazione di responsabilità dell'installatore esterno dell'Istituto scolastico per quel che riguarda le misure minime di sicurezza del trattamento dei dati personali e tra queste quelle previste per le copie di back-up.

Quanto affermato muove dalla considerazione che ogni giorno leggiamo di nuovi virus che si propagano rapidamente e che gli stessi sono causa di notevoli danni che a volte raggiungono proporzioni gigantesche.

Il Dirigente scolastico nella qualità di Titolare del trattamento dei dati personali dell'Istituto Scolastico ha prestato molta attenzione a questo delicato problema ed ha ben ritenuto di prevedere una serie di procedure di recupero immediato dei dati in caso di attacchi e, comunque, delle copie di salvataggio periodiche dei dati personali trattati.

Per il raggiungimento di tale obiettivo sono state correttamente analizzati e testati tutti i software in possesso dell'Istituto scolastico, tutti gli hardware nonché tutti gli altri strumenti informatici tecnico-operativi dell'intero sistema informatico scolastico.

Devesi comunque rilevare che nel campo dell'insegnamento non sono state mai registrate problematiche in ordine al trattamento dei dati personali e ciò nonostante, il Dirigente Scolastico non ha mai tralasciato, comunque, l'aspetto della sicurezza e della protezione dei dati personali per la quale si precisa, pertanto, che già da parecchi anni sono state applicate e predisposte tutta una serie di contromisure e tra queste quelle delle copie di back-up periodiche.

9) Interventi formativi degli incaricati del trattamento.

9.1) Scopo della formazione.

Il dirigente scolastico ha ritenuto che la previsione degli interventi formativi degli incaricati del trattamento rientra tra gli aspetti più importanti del presente documento programmatico sulla sicurezza e ciò in quanto può realmente parlarsi di effettiva sicurezza del trattamento solo in costanza di un dettagliato piano di formazione degli incaricati.

Alla stregua delle altre materie e degli adempimenti previsti a carico del personale insegnante

e non, la formazione è stata ritenuta alla stessa stregua di un elemento fondamentale per il raggiungimento degli obiettivi prefissati ed in particolare per quello della sicurezza del trattamento dei dati personali.

Da quanto evidenziato ne consegue che la predisposizione e l'applicazione di sofisticati strumenti di sicurezza, informatica e non, non garantiscano la stessa in modo assoluto senza le capacità e/o le adeguate conoscenze del personale chiamato alla loro gestione. In effetti, una gestione impropria da parte degli operatori, la mancanza di chiare direttive esplicative e l'assenza di strumenti di controllo di facile e rapida applicazione costituiscono le cause principali per la verificazione anche inconsapevole di danni agli interessati ed in definitiva la causa prioritaria di trattamenti illegittimi.

Quanto premesso trova effettivo riscontro nel comma 19.6. del D.Lgs. 196/2003 che impone, infatti, *"la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare".*

Stesso riscontro all'art. 39, 47 troviamo nel Regolamento UE 2016/679 in cui il Titolare del Trattamento è chiamato a vigilare sulla formazione degli incaricati/autorizzati al trattamento in relazione al trattamento dei dati personali.

La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.

9.2) Tecniche di formazione degli incaricati del trattamento dei dati personali.

Tra gli aspetti salienti della disamina degli interventi formativi degli incaricati del trattamento, il Dirigente scolastico ha ritenuto necessario ed indispensabile prevedere un adeguato e dettagliato piano di formazione degli incaricati del trattamento dei dati personali .

Tale indispensabile strumento sulla sicurezza è articolato in lezioni in ognuna delle quali devono essere affrontati specificamente e dettagliatamente gli aspetti più delicati della legge sulla Privacy e del Regolamento UE e sulle misure di sicurezza e ciò al fine di permetterne vari approfondimenti nonché riflessioni e dibattiti.

Tra le varie tecniche didattiche il Titolare del Trattamento dei dati personali dell'Istituto scolastico ha ritenuto più proficua quella della lezione tenuta direttamente dal Responsabile della protezione dei dati in base alla sua specifica conoscenza della materia della Privacy e ciò con il supporto di materiale cartaceo e/o informatico esplicativo della Legge sul trattamento dei dati personali del quale gli incaricati presenti alle lezioni di formazione dovranno essere corredati al fine della migliore e più completa comprensione della materia e degli adempimenti richiesti dalla medesima nonché delle misure minime di sicurezza applicate dall'Istituto scolastico.

9.3) Valutazione dell'efficienza del piano di formazione

Il Dirigente scolastico ed il Responsabile della protezione dei dati personali dopo avere dettagliatamente individuato il contenuto del piano di formazione hanno ritenuto ulteriormente importante approntare una serie di strumenti di verifica dell'efficienza della formazione per essere certi che la formazione impartita sia stata realmente recepita dagli incaricati del trattamento e che sia stata determinante ad un appropriato e sicuro trattamento dei dati personali.

Si è ritenuto che la formazione possa affermarsi e dirsi veramente tale solo se in grado di soddisfare le esigenze dell'Istituto scolastico per la salvaguardia delle quali è stata prevista

l'utilizzazione di un questionario da sottoporre ai partecipanti a fine corso per effettuare una dettagliata valutazione dell'efficacia del loro apprendimento.

9.4) Aggiornamento e programmi individuali di formazione.

Dopo avere affrontato nel dettaglio l'importanza di tale adempimento deve, comunque, ricordarsi che la formazione deve essere sempre aggiornata. Deve tenersi ben presente una chiara distinzione tra:

A. **AGGIORNAMENTO PERIODICO**
B. **AGGIORNAMENTO SPECIFICO**

L'aggiornamento periodico deve essere adempiuto sotto la diretta vigilanza del Titolare del Trattamento con cadenza almeno annuale e quello specifico, viceversa, tempestivamente effettuato ogni qualvolta l'incaricato sia deputato a trattare nuove banche dati oppure utilizzi nuovi strumenti informatici e/o nuove e/o diverse procedure. L'aggiornamento specifico, altresì, deve essere attivato ogniqualvolta, al manifestarsi di una anomalia grave, il Titolare del trattamento e/o il Responsabile del Trattamento ritenga opportuno effettuare un aggiornamento della formazione e/o dell'informazione degli incaricati.

Muovendo da questa considerazione ne discende che se l'incaricato viene assegnato a nuove mansioni o se viene trasferito da un settore ad un altro deve essere effettuato un nuovo e specifico aggiornamento mediante un programma individuale che deve essere impartito in relazione alla nuova e specifica attività di trattamento svolta.

10) Misure di sicurezza suppletive relative al trattamento di particolari dati sensibili.

Il presente paragrafo evidenzia le ulteriori misure in caso di trattamento di dati particolari o giudiziari ed in particolare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché 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.

Vengono, pertanto, individuati dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Una breve parentesi è necessaria per comprendere nel dettaglio gli adempimenti da effettuarsi ed in particolare un riferimento al punto 20 del disciplinare tecnico secondo quale "*I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all' art. 615- ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici*" ed il successivo punto 21 che stabilisce, inoltre, che *"sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti",* oltre ancora il punto 22 secondo il quale i *supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili".*

Per quanto riportato nel detto disciplinare il punto 23 prescrive che *"sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni".*

Per quanto sopra riportato non v'è dubbio che la protezione crittografica dei dati cui si riferisce lo stesso Testo Unico in materia di trattamento di dati personali rappresenti un prezioso

strumento di tutela e di sicurezza contro i rischi di accesso ai dati personali.

Deve porsi particolare attenzione al trattamento dei dati particolari poiché debbono essere archiviati nel sistema informatico centrale con estrema sicurezza perché l'accesso alla consultazione e/o alla modificazione dei dati particolari sarà sempre condizionato dal rispetto della procedura di identificazione degli incaricati ed in definitiva dei seguenti criteri in base ai quali:

A. **L'incaricato deve essere precisamente individuato ed autenticato;**
B. **L'incaricato può trattare i dati sensibili solo con un appropriato profilo di autorizzazione;**
C. **L'incaricato deve essere in possesso della chiave di lettura o cifratura.**

Per quanto detto e per le menzionate procedure gestionali dei dati particolari deve evidenziarsi in definitiva che i dati particolari debbono essere nettamente separati e gestiti autonomamente ed indipendentemente da ogni incaricato unicamente in base al proprio profilo di autorizzazione.