PIANO PER LA SICUREZZA INFORMATICA, DISASTER RECOVERY E CONTINUITÀ OPERATIVA

Istituto Statale d'Istruzione Superiore "Vincenzo Manzini" di San Daniele del Friuli

SOMMARIO

Sezione A - Introduzione e struttura del documento

Il documento è organizzato in sezioni, punti e tabelle di raccordo. La redazione è ispirata alle regole presenti nel disciplinare tecnico Allegato B D.L. 196/2003, e si prefigge lo scopo di definire le linee guida per lo sviluppo di una serie di attività ed adeguamenti finalizzati al pieno rispetto della normativa.
Il presente documento è frutto di accurate analisi in capo alle infrastrutture, alle situazioni ambientali, agli istituti organizzativi oltre che al personale coinvolto. Il documento Programmatico diverrà infine parte integrante di una più ampia struttura documentale che verrà denominata "Manuale della sicurezza e della privacy".

Ambito di applicazione

Il presente documento si riferisce alle strutture di seguito specificate e definisce lo stato di attuazione in relazione alle disposizioni del Codice in materia di protezione dei dati personali. (Art. 34 e allegato B, regola 19, del D.L. 196/2003).

0000) Sedi del trattamento

Codice	Descrizione	Indirizzo	Città
0001	**Segreteria ISIS "Vincenzo Manzini"**	**Piazza IV Novembre, 4**	**San Daniele del Friuli (UD)**

Titolare del trattamento e firmatario del presente documento è:

Il Dirigente Scolastico pro tempore
dott. Giuseppe Santoro

Digitally signed by Santoro Giuseppe
Date: 2015.11.14 12:16:54 CET

Punto 1) Natura ed elenco dei dati personali (regola 19.1, all. B D. Leg.vo 196/2003)

Di seguito vengono elencate le tipologie di dati personali di cui si gestisce il trattamento per le sedi di tabella 0000.
La descrizione è organizzata in codice progressivo del trattamento, con una breve descrizione dei dati oggetto del trattamento stesso, dei locali in cui avviene e con quali strumenti. In particolare la colonna relativa ai locali riporta i codici di riferimento delle tabelle A103 e A104 nel formato TTTT-CCCC, dove TTTT=tabella e CCCC=codice.

A101) Elenco dei trattamenti informatizzati

Codice	Descrizione sintetica del contenuto dei dati oggetto del trattamento	Codice locali in cui si esegue il trattamento (tab. A103 e A104)	Strumenti elettronici
0001	Anagrafe alunni, in database di Spaggiari SpA e SIDI	A103-0001	PC-LAN, database su server Windows 2007 s.e.
0002	Anagrafe dei tutori, in database di Spaggiari SpA	A103-0001	PC-LAN, database su server Windows 2007 s.e.
0003	Dati curriculari, valutazioni e assenze degli alunni, in database di Spaggiari SpA	A103-0001, A103-0002	PC-LAN, database su server Windows 2007 s.e.
0004	Anagrafe dati del personale, dati di servizio ed assenze, dati retributivi, in database di Spaggiari SpA e SIDI	A103-0001	PC-LAN, database su server Windows 2007 s.e.
0005	Anagrafe dei fornitori e protocollo in database di Spaggiari, posta elettronica	A103-0001	PC-LAN, database su server Windows 2007 s.e.
0006	Verbali delle adunanze degli organi collegiali	A103-0001, A103-0002	PC-LAN, documenti Ms Office
0007	Posta Elettronica Certificata	A103-0001, A103-0002	PC-LAN, documenti Ms Office
0008	Registri Obbligatori segreteria		PC-LAN, documenti Ms Office
0009	Registri obbligatori didattica		PC-LAN, documenti Ms Office e Open Office

Tabella A101 Elenco dei trattamenti informatizzati

La tabella A102 che segue riporta, analogamente alla precedente, l'elenco dei trattamenti effettuati con strumenti diversi da quelli informatici. Si noterà che diversi trattamenti risultano duplicati tra la tabella seguente e quella precedente, ma questa fattispecie è normale laddove si proceda con molteplici strumenti.

A102) Elenco dei trattamenti con strumenti diversi da quelli informatici (regole 27-29, all. B D. Leg.vo 196/2003)

Codice	Descrizione sintetica del contenuto dei dati oggetto del trattamento	Codice locali in cui si esegue il trattamento (tab. A103 e A104)	Strumento e modalità di archiviazione
0001	Informazioni anagrafiche alunni (iscritti prima del 2012)	A103-0001	Cartaceo, fascicoli, faldoni in schedario e armadio
0002	Anagrafe dei tutori (iscritti prima del 2012)	A103-0001	Cartaceo, fascicoli, faldoni in schedario e armadio
0003	Dati curriculari, valutazioni e assenze degli alunni, pagelle, registri generali, del professore e di classe (iscritti prima del 2012)	A103-0001, A103-0002,	Cartaceo, fascicoli, faldoni in schedario e armadio
0004	Anagrafe dati del personale, dati di servizio, dati retributivi	A103-0001	Cartaceo, fascicoli, faldoni in schedario e armadio
0005	Documentazione contabile relativa ai versamenti su ccp e minute spese	A103-0001	Cartaceo, fascicoli, faldoni in schedario e armadio

Tabella A102, Elenco dei trattamenti con strumenti diversi da quelli informatici (regole 27-29, all. B D. L.vo 196/2003)

La tabella A103 riguarda il dettaglio delle strutture di riferimento. Si è proceduto qui alla disamina dei locali ove normalmente si procede al trattamento dei dati specificati sia in tabella A101 che in A102, nel formato TTTT-CCCC, dove TTTT=tabella e CCCC=codice. Per semplicità di gestione ad ogni locale è stato attribuito un codice numerico e nel campo codice sede si fa riferimento alla tabella 0000, che individua l'indirizzo dell'immobile.

A103) Struttura di riferimento

Codice	Descrizione del locale in cui si esegue il trattamento	Codice sede (tab. 0000)
0001	Ufficio del Dirigente	0000-0001
0002	Ufficio Segreteria	0000-0001
0003	Archivio Segreteria	0000-0001
0004	Sala insegnanti	0000-0002

Tabella A103, Struttura di riferimento

Punto 2) Natura ed elenco dei dati sensibili (regola 19.1, all. B D. Leg.vo 196/2003)

Nell'ambito delle attività (tabelle A101 e A102), all'interno della struttura (tabella A103), si procede al trattamento di dati sensibili sanitari, giudiziari e d'iscrizione sindacale. Tali dati sono custoditi in archivio riservato ed in schedari dislocati negli uffici, e comunque in accordo con le procedure presenti nel manuale della Privacy che ha recepito il Regolamento del disciplinare tecnico (All. B, D. Leg.vo 196/2003).

Sezione B Individuazione dei Soggetti con ruoli determinati

Punto 1) Struttura organizzativa funzionale alle attività di trattamento (regola 19.2, all. B D. Leg.vo 196/2003)

Nella tabella B101 vengono elencati i diversi soggetti che allo stato attuale sono individuati come "interessati" da una qualche procedura relativa al trattamento. Per ulteriori dettagli si rimanda a maggiori specificazioni presenti in documentazioni di organigramma, mansionario e/o ordini di servizio, contratti, nomine ed incarichi di responsabilità. Anche per questa tabella si utilizzano dei codici collegamento nel formato TTTT-CCCC, dove TTTT=tabella e CCCC=codice. Il campo gruppo individua genericamente la tipologia di inquadramento del personale interessato.

B101) Soggetti interessati, struttura organizzativa funzionale alle attività di trattamento

Codice	Gruppo	Cognome e Nome	Codici dati trattati	Tipologia trattamento	Responsabilità
0001	==	Dirigente Scolastico	TUTTI	TUTTI	Titolare
0002	==	Dirigente Scolastico e Direttore S.G.A	==	==	Custodia chiavi casseforti
0003	==	Direttore S.G.A.	==	==	Attribuzione e custodia credenziali di accesso
0004	==	Direttore S.G.A.	A101-0001, A102-0001, A101-0002, A102-0002, A101-0003, A102-0003	==	Responsabile
0005	==	Direttore S.G.A.	A101-0004, A102-0004	==	Responsabile
0006	==	Direttore S.G.A.	A101-0005, A102-0007	==	Responsabile
0007	==	Direttore S.G.A.	A102-0003	==	Responsabile
0008	==	Direttore S.G.A.	A101-006, A102-0006	==	Responsabile
0009	==	Direttore S.G.A.	==	==	Amministrazione della rete
0010	==	Direttore S.G.A.	==	==	Procedure di backup/restore
0011	ATA Ass. Amm.	Personale diverso	==	==	Procedure di disaster recovery

0012	ATA segr. didattica	Personale diverso	A101-0001, A102-0001, A101-0002, A102-0002, A101-0003, A102-0003	Inserimento, integrazione, cancellazione	Incaricato
0013	ATA segr. del personale	Personale diverso	A101-0004, A102-0004	Inserimento, integrazione, cancellazione	Incaricato
0014	ATA uff. affari generali	Personale diverso	A101-0005, A102-0007	Inserimento, integrazione, cancellazione	Incaricato
0015	Docenti	Tutti	A102-0003, A102-0006	Inserimento, integrazione, cancellazione e diffusione	Incaricato
0016		Personale diverso	A101-0006, A102-0006	Inserimento, integrazione, cancellazione	Incaricato
0017	==	Personale diverso	==	==	Custodia chiavi locali
0018	==	Personale diverso	==	==	Custodia chiavi armadi e schedari

Tabella B101, Soggetti interessati, Struttura organizzativa funzionale alle attività di trattamento

Punto 2) Amministrazione del sistema informatico

L'incarico di Amministratore del sistema informatico è assegnato al sig. Andrea La Cara.
L'Amministratore produrrà relazioni tecniche delle attività di manutenzione ordinaria e straordinaria.
Il sistema server esegue auditing delle attività dell'Amministratore.
L'Amministratore comunica periodicamente al Titolare dei trattamenti, lo stato e la disponibilità dei files SYSLOG prodotti automaticamente dal server.
L'Amministratore produce inoltre registro verbale delle attività di manutenzione sui sistemi e sulle attività di backup dei dati.

Sezione C Valutazione dei rischi e misure di prevenzione e protezione

Punto 1) Tabella analisi dei rischi (regola 19.3, all. B D. Leg.vo 196/2003)

Nelle tabelle C101, C102 e C103 che seguono si riportano le fattispecie per cui sono evidenziate le vulnerabilità ed il livello di gravità che questi eventi comporterebbero.
Le vulnerabilità sono di 3 tipi:
"NO", per nessuna, "Parziale" e "SI" per vulnerabilità accertata.

Il livello di gravità dell'evento è espresso in 3 gradi:
basso, medio e alto. Per tutti questi rischi si analizzano poi nel punto 2 di questa sezione.

C101) Eventi dovuti a soggetti preposti al trattamento

Codice	Descrizione rischio	Vulnerabilità	Livello di gravità	Danni individuabili
0001	Sottrazione di credenziali di autorizzazione	Parziale	ALTO	Accesso, sottrazione o divulgazione di dati
0002	Carenza di consapevolezza, disattenzione o incuria	No	ALTO	Divulgazione, corruzione o distruzione di dati
0003	Comportamenti sleali o fraudolenti	Parziale	ALTO	Accesso, sottrazione, divulgazione o distruzione di dati
0004	Errore materiale	SI	BASSO	Corruzione o distruzione parziale di dati
0005	Altro evento	SI	Non rilevabile	Non rilevabili

Tabella C101, eventi dovuti a soggetti preposti al trattamento

C102) Eventi relativi agli strumenti del trattamento

Codice	Descrizione rischio	Vulnerabilità	Livello di gravità	Danni individuabili
0001	Azione di virus, worm e male-ware	Parziale	MEDIO	Perdita di file, corruzione ed indisponibilità del sistema
0002	Spamming o tecniche di sabotaggio	Parziale	MEDIO	Perdita di file, corruzione ed indisponibilità del sistema
0003	Malfunzionamento, indisponibilità o degrado degli strumenti	SI	ALTO	Perdita di file, corruzione ed indisponibilità del

				sistema
0004	Accessi esterni non autorizzati	NO	ALTO	Accesso, sottrazione, distruzione o divulgazione di dati
0005	Intercettazioni di informazioni in rete	NO	MEDIO	Accesso o divulgazione di dati
0006	Altro evento	SI	Non rilevabile	Non rilevabili

Tabella C102, Eventi relativi agli strumenti del trattamento

C103) Eventi relativi al contesto fisico-ambientale

Codice	Descrizione rischio	Vulnerabilità	Livello di gravità	Danni individuabili
0001	Accessi non autorizzati a locali/reparti ad accesso ristretto	No	ALTO	Accesso, sottrazione, divulgazione o distruzione di dati
0002	Sottrazione di strumenti contenenti dati	No	ALTO	Accesso, divulgazione o distruzione di dati
0003	Eventi distruttivi naturali o artificiali, nonché dolosi, accidentali o dovuti ad incuria	Parziale	ALTO	Perdita di file, corruzione ed indisponibilità del sistema
0004	Guasto ai sistemi complementari (impianto elettrico, climatizzazione, accessi internet, ecc.)	SI	BASSO	Temporanea indisponibilità del sistema, possibile perdita di dati.
0005	Errori umani nella gestione della sicurezza fisica	Parziale	ALTO	Accesso, divulgazione o distruzione di dati, corruzione ed indisponibilità del sistema
0006	Altro evento	SI	Non rilevabile	Non rilevabili

Tabella C103, Eventi relativi al contesto fisico-ambientale

Punto 2) Misure in essere e di cui si prevede l'adozione (regola 19.4, all. B D. Leg.vo 196/2003)

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 riportate nella tabella seguente, 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.
Le misure sono individuate per tipologia che si presentano come:

- Preventiva laddove si tende a prevenire l'evento dannoso;
- obbligatoria per le misure espressamente definite nel Codice della privacy;
- di contrasto per tutte le misure che inibiscono gli effetti dell'evento dannoso;
- di contenimento degli effetti per le misure che non possono impedire il verificarsi o inibire l'effetto dell'evento dannoso, ma possono almeno ridurne l'entità.

Per definire uno scadenzario degli interventi l'Istituto Scolastico ha adottato un criterio di maggior rilevanza rispetto alle fattispecie di rischio da scongiurare. Questa tabella in particolare sarà oggetto di monitoraggio ed aggiornamento per un miglioramento continuo del sistema di sicurezza, è in tutti i casi sottoposta a revisione annuale o su impulso del Titolare, dei Responsabili o dei Consulenti, laddove si ravvisino necessità di intervento o sopraggiunte non conformità.

C201) Misure in essere e di cui si prevede l'adozione

	Codice	Misure	Tipologia di misura	Rischi contrastati	Trattamenti interessati	Misure già in essere	Misure da adottare	Tempi di adozione/verifica in giorni	Struttura o persona addetta all'adozione
Misure relative agli strumenti	0001	Installazione e configurazione sistema operativo server e client che gestisca le procedure di autenticazione	Preventiva	Accessi indesiderati e non controllati	Tutti	SI	Nessuna	30/30	Amministratore di rete
	0002	Gestione Credenziali di autenticazione a livello di sistema operativo e di procedura gestionale preposta al trattamento	Preventiva	Accessi indesiderati e non controllati	Tutti	Solo password a livello utente senza la gestione delle scadenza e della conformità	Gestione scadenza ed assegnazione credenziali mediante policy di dominio ed eliminazione utenti standard per le procedure gestionali	90/30	Responsabile del trattamento e Amministratore di rete
	0003	Formazione del personale sui rischi, sulle misure disponibili, sulle procedure di conservazione e di ripristino	Obbligatoria	Accessi indesiderati, danneggiamenti o perdita accidentale, applicabilità dell'intero sistema di sicurezza	Tutti	SI	Nessuna	90/30	Responsabile del trattamento

Codice	Misure	Tipologia di misura	Rischi contrastati	Trattamenti interessati	Misure già in essere	Misure da adottare	Tempi di adozione/verifica in giorni	Struttura o persona addetta all'adozione
0004	Antivirus, antispam	Di contrasto	Danneggiamenti o distruzione di dati, indisponibilità dei sistemi	Tutti	SI parziale	Verifica periodica della protezione	90/60	Responsabile del trattamento e Amministratore di rete
0005	Firewall e proxy server	Di contrasto	Danneggiamenti, diffusione o distruzione di dati, indisponibilità dei sistemi	Tutti	SI	Nessuna	90/60	Responsabile del trattamento e Amministratore di rete
0006	Procedure di backup automatizzato	Preventiva	Danneggiamenti o distruzione di dati	Tutti	Si	Verifica periodica della procedura	90/60	Responsabile del trattamento e Amministratore di rete
0007	Procedura per custodia ed uso supporti rimovibili	Contenimento degli effetti	Danneggiamenti o distruzione di dati	Tutti	Custodia in cassaforte	Redazione ed applicazione della procedura	120/60	Responsabile di procedura
0008	Procedure di restore e di disaster recovery	Contenimento degli effetti	Danneggiamenti o distruzione di dati	Tutti	Restore manuale, senza test e procedura per i data base e i documenti in lavorazione	Procedura e test di restore del sistema	90/60	Responsabile del trattamento e Amministratore di rete
0009	Organizzazione delle policy di dominio, gestione dei gruppi organizzativi	Preventiva	Accessi indesiderati e non controllati, danneggiamenti o distruzione	Tutti	Configurazione delle policy e dei gruppi organizzativi	Nessuna	60/30	Responsabile del trattamento e Amministratore di rete

Codice	Misure	Tipologia di misura	Rischi contrastati	Trattamenti interessati	Misure già in essere	Misure da adottare	Tempi di adozione/verifica in giorni	Struttura o persona addetta all'adozione
0010	Sistema di mirroring in RAID	Contenimento degli effetti	Indisponibilità dei sistemi	Tutti	SI	Nessuna	Non def.	Amministratore di rete
0011	Gestione di un server di dominio aggiuntivo o in cluster	Contenimento degli effetti	Indisponibilità dei sistemi	Tutti	Nessuna	Disponibilità pc aggiuntivo, installazione e configurazione	120/60	Amministratore di rete
0012	Attivazione servizi di auditing e monitoraggio	Preventiva	Non tracciabilità di accessi o attività non consentite o fraudolente	Tutti	Nessuna	Attivazione servizi di auditing e monitoraggio	90/60	Amministratore di rete
0013	Procedura di distruzione dei supporti removibili non più in uso	Di contrasto	Diffusione non controllata di dati	Tutti	SI	Nessuna	120/60	Responsabile di procedura
0014	Procedura di spegnimento automatico del server in caso di assenza di alimentazione di rete	Contenimento degli effetti	Danneggiamenti, diffusione o distruzione di dati, indisponibilità dei sistemi	Tutti	SI	Nessuna	90/60	Amministratore di rete
0015	Procedura di sospensione automatica delle sessioni	Preventiva	Accessi indesiderati e non controllati	Tutti	Parzialmente	Attivazione procedura di sospensione automatica su tutti i PC	60/30	Amministratore di rete

	Codice	Misure	Tipologia di misura	Rischi contrastati	Trattamenti interessati	Misure già in essere	Misure da adottare	Tempi di adozione/verifica in giorni	Struttura o persona addetta all'adozione
	0016	Verifica funzionale periodica della funzionalità dei sistemi	Preventiva	Indisponibilità dei sistemi e affidabilità dei dati	Tutti	SI	Verifica funzionale periodica della funzionalità dei sistemi	180/90	Responsabile del trattamento e Amministratore di rete
Misure relative al contesto	0017	Vigilanza attiva della sede	Di contrasto	Accessi indesiderati e non controllati	Tutti	NO	Nessuna	Non def.	Responsabile dei servizi di vigilanza
	0018	Vigilanza passiva della sede	Di contrasto	Accessi indesiderati e non controllati	Tutti	Si, antifurto ad attivazione manuale	Nessuna	Non def.	Responsabile dei servizi di vigilanza
	0019	Registrazione accessi	Preventiva	Accessi indesiderati e non controllati	Tutti	Registro di visita per gli estranei all'amministrazione	Nessuna	180/90	Responsabile dei servizi di vigilanza
	0020	Autenticazione accessi	Di contrasto	Accessi indesiderati e non controllati	Tutti	SI	Nessuna	180/90	Responsabile del trattamento
	0021	Custodia in classificatori ed armadi con chiusura	Preventiva	Accessi indesiderati e non controllati	Tutti	SI	Nessuna	Non def.	Responsabile di procedura
	0022	Deposito in cassaforte o armadi blindati e/o antifiamma	Preventiva	Danneggiamenti o distruzione di dati	Tutti	SI, cassaforte	Nessuna	Non def.	Responsabile di procedura

	Codice	Misure	Tipologia di misura	Rischi contrastati	Trattamenti interessati	Misure già in essere	Misure da adottare	Tempi di adozione/verifica in giorni	Struttura o persona addetta all'adozione
	0023	Dispositivi antincendio	Contenimento degli effetti	Danneggiamenti o distruzione di dati, indisponibilità dei sistemi	Tutti	SI, estintori	Nessuna	Non def.	DSGA o RSPP
	0024	Limitazione dell'accesso dei locali CED o dove risiede il server	Preventiva	Accessi indesiderati e non controllati	Tutti	SI	Nessuna	Non def.	Responsabile dei servizi di vigilanza
Misure relative agli incaricati al trattamento	0025	Assegnazione formale di responsabilità ed incarichi	Obbligatoria	Non applicabilità del sistema di sicurezza	Tutti	In corso di assegnazione a tutto il personale	Nessuna	60/30	Titolare del trattamento
	0026	Certificazione delle attività di società esterne	Obbligatoria	Malfunzionamento o non applicabilità del sistema di sicurezza	Tutti	SI	nessuna	60/30	Responsabile del trattamento
	0027	Formazione per gestione dati con trattamento non informatizzato, finalizzata al controllo degli accessi, alla custodia e conservazione	Obbligatoria	Non applicabilità del sistema di sicurezza	Tutti	SI	Ripetere la sessione di formazione ogni anno	90/30	Titolare del trattamento
	Codice	Misure	Tipologia di	Rischi contrastati	Trattamenti	Misure già in	Misure da	Tempi di	Struttura o

			misura		interessati	essere	adottare	adozione/verifica in giorni	persona addetta all'adozione
	0028	Consultazioni registrate dei dati	Preventiva	Non rintracciabilità degli accessi ai dati	Tutti	SI	Nessuna	90/30	Responsabile del trattamento
	0029	Redazione di elenco strutturato dei dati oggetto del trattamento diviso per classi e finalità di gestione	Obbligatoria	Non applicabilità del sistema di sicurezza	Tutti	Redazione di elenco strutturato dei dati oggetto del trattamento diviso per classi e finalità di gestione	Nessuna	90/30	Responsabile del trattamento
	0030	Procedure di restore e di disaster recovery	Contenimento degli effetti	Danneggiamenti o distruzione di dati	Tutti	Restore automatico a norma dei dati inseriti in Archibox®	Nessuna	30/30	Responsabile del trattamento e Amministratore di rete
	031	Adozione di un Manuale di gestione documentale	Obbligatoria	Malfunzionamento della gestione amministrativa	Tutti	SI	In attesa di approvazione	60/30	Titolare del trattamento
	033	Adozione del Manuale di conservazione sostitutiva	Obbligatoria	Rischio di perdita dei documenti	Tutti	SI	In attesa di approvazione	60/30	Titolare del trattamento

Tabella C201, Misure in essere e di cui si prevede l'adozione

Punto 3) Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5, all. B D. L.vo 196/2003)

Codice Base dati	Criteri e procedure per il salvataggio	Supporto magnetico/ottico e luogo di custodia delle copie	Struttura o persona incaricata del salvataggio	Procedura di ripristino e pianificazione
0001	Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente sulla base di procedura scritta	Salvataggio in cartella del server e replicati su 2 HD drive esterni per base dati in locale	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0002	Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente, sulla base di procedura scritta	Salvataggio in cartella del server e replicati su 2 HD drive esterni	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0003	Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente, sulla base di procedura scritta	Salvataggio in cartella del server e replicati su 2 HD drive esterni	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0004	Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente, sulla base di procedura scritta	Salvataggio in cartella del server e replicati su 2 HD drive esterni	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0005	Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente, nessuna procedura scritta	Salvataggio in cartella del server e replicati su 2 HD drive esterni	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0006	Procedura backup di con cadenza periodica impostata a parametro in	Salvataggio in cartella del server e replicati su 2 HD drive esterni	Amministratore dei sistemi	Restore dati, nessuna pianificazione o

	giorni da ultimo salvataggio. Valore variabile impostato dall'utente, nessuna procedura scritta			test di funzionamento
0007	Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente, nessuna procedura scritta	Salvataggio in cartella del server e replicati su 2 HD drive esterni	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0008	Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente, nessuna procedura scritta	Salvataggio in cartella del server e replicati su 2 HD drive esterni	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0009	Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente, nessuna procedura scritta	Salvataggio in cartella del server e replicati su 2 HD drive esterni	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento

Tabella C301, criteri e modalità di ripristino della disponibilità dei dati

Sezione D Piano di sicurezza informatica (PSI), Disaster recovery (DR) e continuità operativa (CO)

La Direttiva del 16 gennaio 2002 dal titolo "Sicurezza informatica e delle Telecomunicazioni nelle PA statali" raccomanda a tutti gli organi pubblici l'adozione di misure minime di sicurezza, tali da garantire la tutela del loro patrimonio informativo.
Il piano di sicurezza informatica è lo strumento strategico fondamentale per tutelare il sistema informativo, le capacità operative dell'ISIS "V. Manzini", la sua immagine, la produttività degli operatori e il rispetto degli obblighi di legge.
Gli obiettivi che si vogliono conseguire sono di garantire, in accordo con le leggi e le regole interne:

a) per le risorse tecnologiche:
   - la disponibilità del servizio in una forma adeguata, anche a fronte di eventi eccezionali, tramite la formulazione di appropriati piani di recupero delle funzionalità del sistema;
   - la continuità del servizio a copertura delle esigenze operative della scuola.
b) per i dati:
   - la riservatezza delle informazioni;
   - l'integrità delle informazioni;
   - la correttezza delle informazioni ritenute critiche per le eventuali conseguenze derivanti da una loro alterazione;
   - la disponibilità delle informazioni e delle relative applicazioni.

Per risorse informatiche da considerare nell'ambito della sicurezza, ci si riferisce a:

- dispositivi tecnologici (computer, terminali, linee di comunicazione, ...) il cui danneggiamento fisico può comportare l'interruzione del corretto funzionamento e la conseguente sospensione del servizio;
- sistemi operativi o prodotti software la cui modifica, cancellazione o indisponibilità può comportare l'interruzione del funzionamento e la conseguente sospensione del servizio oppure può comportare la possibilità di accesso e manomissione di dati riservati da parte di personale non autorizzato;
- programmi applicativi la cui modifica o cancellazione può compromettere l'esercizio di alcune funzioni del sistema informativo o alterarne le corrette caratteristiche di funzionamento;
- dati per i quali si richiedono riservatezza, integrità e disponibilità.

Il Codice dell'Amministrazione Digitale contiene disposizioni importanti relative alla sicurezza digitale, dei sistemi e delle infrastrutture delle PP. AA. (art.51) rimarcando l'importanza di adottare soluzioni di Continuità Operativa e di Disaster Recovery nella gestione dei sistemi operativi automatizzati. I due termini sembrano molto simili, ma vi è una differenza sostanziale, in quanto la prima è riferita all'organizzazione nel suo insieme (e quindi comprende anche le risorse umane, logistiche, i rischi ambientali, ecc.), mentre la seconda è riferita all'infrastruttura tecnico/informatica.

Punto 1) Procedure di Disaster Recovery (ai sensi del c.3, lettera b) dell'art. 50bis del Codice dell'Amministrazione Digitale)

Le Pubbliche Amministrazioni devono predisporre appositi piani di emergenza idonei ad assicurare, in caso di eventi disastrosi, la continuità delle operazioni indispensabili a fornire i servizi e il ritorno alla normale operatività.

Per Disaster Recovery si intende quindi l'insieme di misure tecnologiche e organizzative dirette a ripristinare, sistemi, dati e infrastrutture necessarie all'erogazione di servizi a fronte di gravi emergenze. I disastri informatici con ingenti perdite di dati nella maggioranza dei casi provocano quindi il fallimento dell'organizzazione, per cui investire in opportune strategie di recupero diventa una scelta quasi obbligatoria e il Piano di disaster recovery è il documento che esplicita tali misure.
L'attività di backup è un aspetto fondamentale della gestione del sistema informatico dell'ISIS "V. Manzini": in caso di guasti, manomissioni, furti, ecc., assicura che esista una copia dei dati, garantendo quindi una ridondanza logico/fisica dei dati. Si tratta di una misura tipica delle procedure di disaster recovery.
L'ISIS "V. Manzini" utilizza sistemi di backup differenti: uno on-site e sempre on-line per i trattamenti informatizzati attraverso gli applicativi in uso (database software gestionale scolastico Axios-Infoschool) e uno off-line su supporto removibile esterno.
Il backup on-site è effettuato sul server presente nella scuola. L'esecuzione del backup è impostata in maniera automatica e svolta con una periodicità stabilita di una volta al giorno. In particolare, il software utilizzato è l'utility di backup del software gestionale scolastico Axios-Infoschool ed è programmato per svolgere il backup giornaliero e differenziato.
Il backup giornaliero esegue giornalmente una copia dei dati nella cartella StoreBackup del database del software gestionale scolastico:

C:\AxiosSpa\Dati

Il backup è schedulato in automatico per giorni della settimana a un determinato orario. Il software utilizzato crea nella cartella di destinazione degli archivi nominati con il giorno della settimana.
Un terzo tipo di Backup viene salvato nella cartella ManualBackup e viene eseguito manualmente dall'operatore incaricato prima di ogni aggiornamento del software gestionale scolastico Axios-Infoschool.

Punto 2) Continuità Operativa (ai sensi dell'art. 50bis del Codice dell'Amministrazione Digitale)

La Continuità Operativa è essenzialmente il risultato di un processo organizzativo che si avvale di tecnologie informatiche, che non sono diverse da quelle normalmente utilizzate dall'ISIS "V. Manzini" e delle risorse (personale, impianti...) necessarie per il suo funzionamento.
L'ISIS "V. Manzini" ha adottato misure in applicazione del piano di continuità operativa tra cui rivestono particolare importanza i mezzi hardware e software per le repliche remote dei dati e le reti di comunicazione tra i siti principale e di backup:

- server: server alloggiato in apposito locale, dotato di due hard disk con sistema RAID, con caratteristiche di sicurezza e di impianti di raffreddamento molto ridotte o nulle;
- gruppi di continuità (UPS) collegati ai server
- sistema antincendio

Sezione E - Interventi formativi ed altre incombenze

Punto 1) Natura e pianificazione degli interventi formativi (regola 19.6, all. B D. Leg.vo 196/2003)

Il Titolare dei trattamenti stabilisce di organizzare una sessione di base per la formazione al personale attualmente in servizio, mentre si predispone un calendario annuale perenne di formazione per i casi di ingresso al servizio, cambiamento di mansioni, introduzione di nuovi e significativi strumenti.

D101) Natura e pianificazione degli interventi formativi

Brevi cenni sui contenuti	Soggetti interessati e classi di incarico	Durata	Sessioni previste
Panoramica sui rischi, misure disponibili per prevenire eventi dannosi, disciplina della protezione e delle responsabilità che ne derivano.	Responsabile ed Incaricati	2 ore	Almeno una all'anno
Idem	Incaricato di nuovo ingresso al servizio, cambiamento di mansioni, introduzione di nuovi e significativi strumenti.	2 ore	Almeno una all'anno

Tabella D101, natura e pianificazione degli interventi formativi

Punto 2) Trattamenti affidati all'esterno (regola 19.7, all. B D. Leg.vo 196/2003)

Allo stato attuale non vi sono in corso contratti di affidamento di trattamento dati all'esterno della struttura.
Si trasmettono dati solo in ragione dell'esecuzione di normali attività di comunicazione e/o dichiarazione relative ad adempimenti amministrativi, fiscali, quali ad esempio l'utilizzo dei software e/o applicativi web di SIDI, INPS, INAIL, ENTRATEL, ecc.

Punto 3) Cifratura dei dati o separazione di quelli identificativi (reg. 19.8, all. B D. Lg.vo 196/2003)

Nelle basi dati definite in tabelle A101 e A102, si ravvisa la fattispecie indicata nella citata regola 19.8, e si stabilisce di adottare pertanto alcune misure di cifratura e/o organizzative, quali ad esempio l'archiviazione separata ed in contenitore apposito di dati sensibili di utenti, clienti e dipendenti ancorché disponibili nei fascicoli degli stessi e/o in protocollo riservato. L'accesso ai dati sensibili può avvenire solo da parte di soggetti espressamente incaricati e per soli motivi di assoluta necessità in accordo con le prerogative funzionali presenti in apposite procedure del Manuale della Privacy.

Punto 4) Ulteriori misure in caso di trattamento di dati sensibili o giudiziari(regole 20-25, all. B D. Leg.vo 196/2003)

Nell'ambito delle attività che si svolgono all'interno della struttura, si procede al trattamento di dati sensibili come dichiarato nella sezione A punto 2.

Punto 5) Misure di tutela e garanzia (regola 25, all. B D. Lg.vo 196/2003)

In sede di aggiudicazione di appalto di forniture e/o servizi a soggetti esterni, inerenti strumenti per il trattamento dei dati per i quali il Titolare adotta le misure minime di sicurezza, si richiede a detti soggetti, una descrizione scritta dell'intervento/fornitura effettuata, che ne attesta la conformità al disciplinare tecnico Allegato B, D. Leg.vo 196/2003. A tal scopo si allega al presente documento il modello standard di richiesta di dichiarazione. (MOD1960001.RTF)

Questo documento è suscettibile di revisione annuale entro il 31 marzo, e tutte le volte che il Titolare del trattamento ne ravvisi la necessità.

San Daniele del Friuli, 14 novembre 2015

Il titolare dei trattamenti
Il Dirigente Scolastico
dott. Giuseppe Santoro

Allegati:

Codice della privacy D.L.vo 196/03
MOD1960001.RTF (richiesta di certificato di conformità al fornitore)
MOD1960002.RTF (certificato di conformità del fornitore)
MOD1960003.RTF (nomina del Responsabile del trattamento)
MOD1960004.RTF (nomina dell'Incaricato del trattamento)
MOD1960005.RTF (nomina di Responsabili esterni del trattamento)
MOD1960006.RTF (nomina del Responsabile per l'accesso ai locali)
MOD1960007.RTF (procedura di accesso ai dati da parte dell'interessato)
MOD1960008.RTF (modulo per l'esercizio dei diritti da parte dell'interessato)
MOD1960009.RTF (modulo per le informative)
MOD1960010.RTF (modulo per la richiesta del consenso al trattamento)
MOD1960011.RTF (modulo rapporto di non conformità)
MOD1960012.RTF (modulo accesso strumenti informatici)