Ministero dell'Istruzione, dell'Università e della Ricerca
Istituto Comprensivo Statale "G.Rodari"
Via Aquileia, 1 – 20021 Baranzate (MI)
Tel/fax 02-3561839
Cod. Fiscale 80126410150 Cod. meccanografico MIIC8A900C
e-mail: miic8a900c@istruzione.it **– pec:** miic8a900c@pec.istruzione.it

DOCUMENTO PROGRAMMATICO PER LA SICUREZZA E LA TUTELA DELLA PRIVACY

(D.Lgs. 196 del 30 giugno 2003 – Codice in materia di protezione dei dati personali)

PIANO PER LA SICUREZZA INFORMATICA, DISASTER RECOVERY E CONTINUITÀ OPERATIVA

(Art. 50bis del D.Lgs. 82 del 7 marzo 2005 – Codice dell'Amministrazione Digitale)

Versione 4 gennaio 2021

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.Lgs. 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.

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.Lgs. 196/2003).

0000) Sedi del trattamento

Codice	Descrizione	Indirizzo	Città
0001	Sede – IC Rodari	Via Aquileia 1	Baranzate (MI)
0002	Scuola primaria "G. Rodari"	Via Mentana	Baranzate (MI)
0003	Scuola infanzia "C. Collodi"	Via Salvo D'Acquisto	Baranzate (MI)
0004	Scuola infanzia "Marco Polo"	Via Mercantesse	Baranzate (MI)
0005	Scuola infanzia "Sant'Arialdo"	Via Fiume 14	Baranzate (MI)

Titolare del trattamento e firmatario del presente documento è:

Il Dirigente Scolastico pro tempore dott. Marco Paolo Morini

Punto 1) Natura ed elenco dei dati personali (regola 19.1, all. B D.Lgs. 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 della tabella A103 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)	Strumenti elettronici
0001	Anagrafe alunni	A103-0001, A103-0002, A103-0003	PC-LAN, database Sybase per programma AXIOS/SISSI, programma AXIOS/Segreteria Digitale, Server XP Home Edition + XP Professional
0002	Anagrafe dei tutori	A103-0001, A103-0002,	PC-LAN, database Sybase per programma

		A103-0003	AXIOS/SISSI, programma AXIOS/Segreteria Digitale, Server XP Home Edition + XP Professional
0003	Dati curriculari, valutazioni e assenze degli alunni	A103-0001, A103-0002, A103-0003, A103-0004, A103-0005, A103-0006, A103-0007, A103-0008	PC-LAN, database Sybase per programma AXIOS/SISSI, programma AXIOS/Segreteria Digitale, programma AXIOS/Registro Elettronico, Server XP Home Edition + XP Professional
0004	Anagrafe dati del personale, dati di servizio ed assenze, dati retributivi e contabili	A103-0001, A103-0002, A103-0003	PC-LAN, database Sybase per programma AXIOS/SISSI, programma AXIOS/Segreteria Digitale, Server XP Home Edition + XP Professional
0005	Anagrafe dei fornitori	A103-0001, A103-0002, A103-0003	PC-LAN, programma AXIOS/Segreteria Digitale
0006	Protocollo Informatico	A103-0002, A103-0003	PC-LAN, programma AXIOS/Protocollo Web, programma AXIOS/Segreteria Digitale
0007	Verbali delle adunanze degli organi collegiali	A103-0001, A103-0002, A103-0003, A103-0004, A103-0005, A103-0006, A103-0007, A103-0008	PC-LAN, documenti MS Office, programma AXIOS/Segreteria Digitale
0008	Gestione delle caselle di Posta Elettronica e Posta Elettronica Certificata	A103-0001, A103-0002, A103-0003	PC-LAN, client di posta, programma AXIOS/Segreteria Digitale

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.Lgs. 196/2003)

Codice	**Descrizione sintetica del contenuto dei dati oggetto del trattamento**	**Codice locali in cui si esegue il trattamento (tab. A103)**	**Strumento e modalità di archiviazione**
0001	Informazioni anagrafiche alunni (iscritti prima del 2012 e scuola infanzia)	A103-0003	Cartaceo, fascicoli, faldoni in schedario e armadio
0002	Anagrafe dei tutori (iscritti prima del 2012 e scuola infanzia)	A103-0003	Cartaceo, fascicoli, faldoni in schedario e armadio
0003	Dati curriculari, valutazioni e assenze degli alunni, registri del professore e di classe	A103-0003, A103-0004, A103-0005, A103-0006, A103-0007, A103-0008	Cartaceo, fascicoli, faldoni in schedario e armadio
0004	Anagrafe dati del personale, dati di servizio ed assenze, dati retributivi e contabili	A103-0003	Cartaceo, fascicoli, faldoni in schedario e armadio
0005	Verbale delle adunanze degli organi collegiali	A103-0001, A103-0003, A103-0004, A103-0005, A103-0006,	Cartaceo, fascicoli, faldoni in schedario e

		A103-0007, A103-0008	armadio

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 del D.S.G.A.	0000-0001
0003	Ufficio di Segreteria	0000-0001
0004	Sala insegnanti secondaria Galilei	0000-0001
0005	Sala insegnanti primaria Mentana	0000-0002
0006	Sala insegnanti Infanzia Collodi	0000-0003
0007	Sala insegnanti infanzia Marco Polo	0000-0004
0008	Sala insegnanti infanzia Sant'Arialdo	0000-0005

Punto 2) Natura ed elenco dei dati sensibili (regola 19.1, all. B D.Lg.s 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 Ministero della Pubblica Istruzione (Decreto 305/2006 e relative schede) in materia di trattamento di dati sensibili e giudiziari.

Sezione B Individuazione dei Soggetti con ruoli determinati

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

Nella tabella A104 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 sig. Morini Marco Paolo	TUTTI	TUTTI	Titolare
0002	==	Dirigente Scolastico sig. Morini Marco Paolo e Direttore S.G.A. sig.re Ornella Dimunno	==	==	Custodia chiavi casseforti
0003	==	Direttore S.G.A. sig.ra Ornalla Dimunno	==	==	Attribuzione e custodia credenziali di accesso
0004	==	Direttore S.G.A.	==	==	Responsabile
0005	==	Direttore S.G.A.	==	==	Amministrazione della rete
0006	==	Direttore S.G.A.	==	==	Procedure di backup/restore
0007	ATA Assistenti Amm.inistrativi	Personale diverso	==	==	Procedure di disaster recovery
0008	ATA segreteria didattica	Personale diverso	A101-0001, A102-0001, A101-0002, A102-0002, A101-0003, A102-0003	Inserimento, integrazione, cancellazione	Incaricato
0009	ATA segreteria del personale	Personale diverso	A101-0004, A102-0004	Inserimento, integrazione, cancellazione	Incaricato
0010	ATA ufficio affari generali	Personale diverso	A101-0005	Inserimento, integrazione, cancellazione	Incaricato
0011	Docenti	Tutti	A101-0003, A102-0003, A101-0007,	Inserimento, integrazione, cancellazione e	Incaricato

			A102-0005	diffusione	
0012	==	Personale diverso	A101-0006, A101-0008	Inserimento, integrazione, cancellazione	Incaricato
0013	==	Personale diverso	==	==	Custodia chiavi locali
0014	==	Personale diverso	==	==	Custodia chiavi armadi e schedari

Punto 2) Amministrazione del sistema informatico

L'incarico di Amministratore del sistema informatico è assegnato al DSGA Sig.ra Ornella Dimunno. 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.Lgs. 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"
- "SI" per vulnerabilità accertata.

Il livello di gravità dell'evento è espresso in 3 gradi: basso, medio e alto. 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	SI	ALTO	Accesso, sottrazione o divulgazione di dati
0002	Carenza di consapevolezza, disattenzione o incuria	SI	ALTO	Divulgazione, corruzione o distruzione di dati
0003	Comportamenti sleali o fraudolenti	SI	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

C102) Eventi relativi agli strumenti del trattamento

Codice	Descrizione rischio	Vulnerabilità	Livello di gravità	Danni individuabili
0001	Azione di virus, worm e malware	Parziale	MEDIO	Perdita di file, corruzione ed indisponibilità del sistema
0002	Spamming o tecniche di sabotaggio	SI	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	SI	ALTO	Accesso, sottrazione, distruzione o divulgazione di dati
0005	Intercettazioni di informazioni in rete	SI	MEDIO	Accesso o divulgazione di dati
0006	Altro evento	Parziale	Non rilevabile	Non rilevabili

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	Parziale	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.)	Parziale	BASSO	Temporanea indisponibilità del sistema, possibile perdita di dati.
0005	Errori umani nella gestione della sicurezza fisica	SI	ALTO	Accesso, divulgazione o distruzione di dati, corruzione ed indisponibilità del sistema
0006	Altro evento	SI	Non rilevabile	Non rilevabili

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

Dopo aver analizzato e valutato i fattori di rischio, relativi alle aree e ai 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	90/30	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	Sì	Nessuna	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	No	Da programmare	90/30	Responsabile del trattamento
	0004	Antivirus, antispam	Di contrasto	Danneggiamenti o distruzione di dati,	Tutti	SI	Nessuna	90/60	Responsabile del trattamento

				indisponibilità dei sistemi					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	Backup automatico ogni sera	Nessuna	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	No	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 database 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	Sì	Nessuna	60/30	Responsabile del trattamento e Amministratore di rete
	0010	Sistema di mirroring in	Contenimento degli effetti	Indisponibilità dei sistemi	Tutti	SI	Nessuna	Non definiti	Amministratore di rete

		RAID							
	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	Sì	Nessuna	90/60	Amministratore di rete
	0013	Procedura di distruzione dei supporti removibili non più in uso	Di contrasto	Diffusione non controllata di dati	Tutti	No	Attivazione procedura di distruzione dei supporti removibili non più in uso	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	No	Installazione e configurazione di apparecchiatura di intervento automatico	90/60	Amministratore di rete
	0015	Procedura di sospensione automatica delle sessioni	Preventiva	Accessi indesiderati e non controllati	Tutti	Sì	Nessuna	60/30	Amministratore di rete
	0016	Verifica funzionale periodica della funzionalità dei sistemi	Preventiva	Indisponibilità dei sistemi e affidabilità dei dati	Tutti	SI	Nessuna	180/90	Responsabile del trattamento e Amministratore di rete
Misure	0017	Vigilanza attiva della sede	Di contrasto	Accessi indesiderati e non controllati	Tutti	Sì	Nessuna	Non definite	Responsabile dei servizi di vigilanza

	0018	Vigilanza passiva della sede	Di contrasto	Accessi indesiderati e non controllati	Tutti	Sì	Nessuna	Non definiti	Responsabile dei servizi di vigilanza
	0019	Registrazione accessi	Preventiva	Accessi indesiderati e non controllati	Tutti	Sì	Istituire un registro di visita per gli estranei all'amministrazione	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 definiti	Responsabile di procedura
	0022	Deposito in cassaforte o armadi blindati e/o antifiamma	Preventiva	Danneggiamenti o distruzione di dati	Tutti	SI	Nessuna	Non definiti	Responsabile di procedura
	0023	Dispositivi antincendio	Contenimento degli effetti	Danneggiamenti o distruzione di dati, indisponibilità dei sistemi	Tutti	SI, estintori e impianto di allarme	Nessuna	Non definiti	DSGA o RSPP
	0024	Limitazione dell'accesso dei locali CED o dove risiede il server	Preventiva	Accessi indesiderati e non controllati	Tutti	No	Rilevazione ed autenticazione mediante autorizzazioni	Non definiti	Responsabile dei servizi di vigilanza
Misure relative agli	0025	Assegnazione formale di responsabilità ed incarichi	Obbligatoria	Non applicabilità del sistema di sicurezza	Tutti	Sì	Nessuna	60/30	Titolare del trattamento
	0026	Certificazione delle attività di società esterne	Obbligatoria	Malfunzionamento o non applicabilità del sistema di sicurezza	Tutti	NO	Inviare lettera di richiesta del certificato	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	No	Ripetere la sessione di formazione ogni anno	90/30	Titolare del trattamento
	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	NO	Redazione di elenco strutturato dei dati oggetto del trattamento diviso per classi e finalità di gestione	90/30	Responsabile del trattamento
	0030	Procedure di restore e di disaster recovery	Contenimento degli effetti	Danneggiamenti o distruzione di dati	Tutti	NO	Restore automatico a norma dei dati	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	Nessuna	60/30	Titolare del trattamento

Punto 3) Criteri e modalità di ripristino della disponibilità dei dati (regola 19.5, all. B D.Lgs. 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 Axios/Sissi con cadenza periodica impostata manualmente	Salvataggio in cartella del server	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0002	Procedura backup dei documenti Office, dei database della posta elettronica e cartelle condivise con cadenza giornaliera automatica.	Salvataggio in HD drive esterno collocato in ufficio DSGA	Amministratore dei sistemi	Restore dati, nessuna pianificazione o test di funzionamento
0003	Salvataggio in cloud in tempo reale del database di registro elettronico	Salvataggio in cloud https://re26.axioscloud.it gestito da Axios Italia Service s.r.l.	Automatico	
0004	Salvataggio in conservazione sostituiva ai sensi del DPCM 03/12/2013	Conservazione a norma con contratto con Axios Italia Service s.r.l. e soggetto conservatore 2C Solution s.r.l.	Personale vario	Funzionalità di ricerca, consultazione ed esibizione dei dati descritte nel manuale di conservazione

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'I.C. Rodari, 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:

- 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.
- 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'I.C. Rodari: 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'I.C. Rodari utilizza sistemi di backup differenti per tipologia di dati: uno on-site per i trattamenti informatizzati attraverso gli applicativi in uso (database) e uno out-site per i trattamenti di cui si effettua la conservazione sostitutiva ai sensi del DPCM del 03/12/2013.

Il backup on-site è effettuato sul server presente nell'ufficio di Segreteria e su hard disk esterno. L'esecuzione del backup è impostata in maniera automatica e svolta con una periodicità stabilita di una volta al giorno. Il backup giornaliero esegue giornalmente una copia dei dati nell'apposito sistema esterno (hard disk rimovibile collocato in locale distinto da quello in cui è posto il server) di tutte le cartelle presenti sul server. Il backup è schedulato in automatico per giorni della settimana (dal lunedì al venerdì) alle ore 20.00. Il software utilizzato crea nella cartella di destinazione delle cartelle nominate per giorno della settimana e ricrea l'intero percorso degli elementi copiati.

Il backup on-site dei database del sistema Axios/SISSI viene effettuato periodicamente sul server in occasione degli aggiornamenti del sistema e in altre evenienze, con attivazione manuale.

Il backup out-site si avvale del servizio di conservazione sostituiva a norma fornito dalla società 2C Solution s.r.l. attraverso contratto con Axios Italia Service s.r.l.

L'I.C. Rodari garantisce che solo gli utenti autorizzati abbiamo la possibilità di vedere in chiaro i dati e i documenti contenuti all'interno del server. Questo livello assicura la privacy sui dati e sui documenti.

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'I.C. Rodari e delle risorse (personale, impianti ...) necessarie per il suo funzionamento.

L'I.C. Rodari 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. La continuità operativa è garantita dal gruppo di continuità collegato al server e dal sistema antincendio e antintrusione dell'edificio sede dell'Istituto.

Punto 3) Sicurezza logica

La sicurezza logica si realizza principalmente assicurando che tutti gli accessi ai diversi componenti del sistema informativo avvengano esclusivamente secondo modalità prestabilite. Per tale motivo, ogni qual volta si rende necessario l'utilizzo di una risorsa, deve essere previsto un meccanismo che costringa l'utente ad autenticarsi, ossia a dimostrare la propria identità, mediante tipicamente l'utilizzo di un codice identificativo personale (*userid*) ed una parola chiave (*password*).

Tutti gli utenti rispettano le seguenti disposizioni:

a) L'utente è responsabile della corretta tenuta della password di accensione del PC che gli è stato assegnato e delle password di accesso alla rete e alle applicazioni;
b) L'utente a cui è stata assegnata una userid per l'accesso alla rete e/o per l'utilizzo di applicazioni informatiche centralizzate, è responsabile di tutto quanto accade a seguito di transazioni ed elaborazioni abilitate dal proprio codice identificativo personale. Per le applicazioni informatiche

centralizzate, tale responsabilità si riferisce ai privilegi associati al suo profilo di abilitazione;

c) L'utente cambia le proprie password secondo le disposizioni riportate nelle misure minime e nel presente manuale;
d) L'utente gestisce le proprie password secondo le disposizioni riportate nelle misure minime e nel presente manuale;
e) L'utente attiva tutte le misure in suo potere per evitare che terzi abbiano accesso al suo PC mentre si allontana durante una sessione di lavoro. A tal fine esce sempre dall'applicazione in uso (*logoff*) ed eventualmente blocca il PC con la password di uno *screen saver*;
f) L'utente non comunica le proprie password esclusivamente al Responsabile della gestione documentale (o al suo delegato) come misura minima per consentire la prosecuzione delle attività amministrative in caso di assenza prolungata dell'utente.

Nell'ambito delle presenti misure minime, sono individuati i seguenti livelli di protezione:

- password di accensione del PC;
- *userid* e *password* per l'accesso alle risorse di rete;
- *userid*, *password* e profili di abilitazione per le applicazioni informatiche centralizzate.

Il Responsabile della gestione documentale mantiene aggiornato un registro cartaceo delle password e dei profili di abilitazione per le applicazioni informatiche, conservato in cassaforte.

Linee guida per il corretto utilizzo delle password

Vi sono diverse categorie di password, ognuna con il proprio ruolo preciso:

a) **la password di accensione del PC** impedisce l'utilizzo improprio della propria postazione di lavoro, quando per un qualsiasi motivo non ci si trova in Ufficio. La password di accensione deve avere una lunghezza non inferiore a **6 caratteri** e deve essere aggiornata almeno ogni **6 mesi**;
b) **la password di rete** impedisce che l'eventuale accesso non autorizzato ad un PC renda disponibili le risorse dell'Ufficio (stampanti, cartelle condivise). La password di rete deve avere una lunghezza non inferiore a **8 caratteri** e deve essere aggiornata almeno ogni **3 mesi**;
c) **la password delle applicazioni informatiche centralizzate** permette di restringere l'accesso alle funzioni e ai dati al solo personale autorizzato. Per la lunghezza delle password delle applicazioni informatiche centralizzate e per la frequenza di aggiornamento, fare riferimento ai manuali delle singole applicazioni;
d) **la password della casella di posta elettronica istituzionale** impedisce che i messaggi di posta elettronica indirizzati ad un utente possano essere letti da utenti non autorizzati;
e) **la password del salvaschermo** impedisce che un'assenza momentanea permetta a una persona non autorizzata di visualizzare il lavoro in corso e/o di accedere ai documenti residenti sulla postazione di lavoro.

La scelta della password da parte dell'utente deve essere oculata in quanto il modo più semplice e più utilizzato per realizzare un accesso illecito ad un sistema e/o ad un applicazione, consiste nell'ottenere le credenziali identificative di un utente autorizzato, ossia la sua coppia *userid* e *password*. Considerato che per molte applicazioni informatiche centralizzate, lo *userid* coincide con dati anagrafici del dipendente ed è quindi un dato noto, l'intera sicurezza si basa sulla conoscenza della *password*. La scelta, quindi, di password "forti" rappresenta un aspetto essenziale della sicurezza informatica.

Nella gestione delle password è necessario attenersi alle indicazioni di seguito riportate.

Cosa NON fare

a) NON comunicare a NESSUNO le proprie password, qualunque sia il mezzo che viene utilizzato per

inoltrare la richiesta (telefono, messaggio di posta elettronica, ecc.). Ricordare che NESSUNO è autorizzato a richiedere le password, nemmeno il personale tecnico di supporto, e che lo scopo principale per cui sono utilizzate le password è di assicurare che nessun altro possa utilizzare le risorse a cui si è abilitati; unica eccezione a questa regola è la comunicazione al Responsabile della gestione documentale delle password necessarie a garantire la continuità della funzionalità degli uffici in caso di propria assenza;

b) NON scrivere le password su supporti che possano essere trovati facilmente e/o soprattutto in prossimità della postazione di lavoro utilizzata;
c) NON scegliere password corrispondenti a parole presenti in un dizionario, sia della lingua italiana che di lingue straniere. Esistono programmi che permettono di provare come password tutte quelle contenute in dizionari elettronici estremamente ampi, in termini di numero di lemmi, e in diverse lingue, scritte sia in senso normale che in senso inverso;
d) NON usare come password il nome utente o parole che possano essere facilmente riconducibili all'identità dell'utente, come, ad esempio, il codice fiscale, il nome del coniuge, il nome dei figli, la data di nascita, il numero di telefono, la targa della propria auto, il nome della strada in cui si abita, il nome della squadra di calcio per cui si tifa, ecc.;
e) NON usare come password parole ottenute da una combinazione di tasti vicini sulla tastiera o sequenze di caratteri (esempio: qwerty, asdfgh, 123321, aaabbb, ecc.);
f) NON usare la STESSA password per le diverse tipologie di password prima individuate;
g) NON rendere note password vecchie e non più in uso, in quanto da questi dati è possibile ricavare informazioni su ciclicità e/o regole empiriche e personali che l'utente utilizza per generare le proprie password.

Cosa FARE

a) Cambiare le password frequentemente ricordando che il limite massimo di validità di una password stabilito dalle presenti misure minime è di 6 mesi (password di accensione del PC);
b) Utilizzare password lunghe almeno otto caratteri con un misto di lettere, numeri e segni di interpunzione;
c) Nella digitazione delle password assicurarsi che non ci sia nessuno che osservi ciò che si digita sulla tastiera del PC;
d) Utilizzare password distinte per le diverse tipologie di password prima descritte.

Come scegliere le password

Le password migliori sono quelle facili da ricordare ma, allo stesso tempo, difficili da individuare. Questo genere di password può essere ottenuto, ad esempio, comprimendo frasi lunghe in pochi caratteri presenti nella frase, utilizzando anche segni di interpunzione e caratteri maiuscoli e minuscoli. La frase "Nel 1969 l'uomo è andato sulla luna" può, ad esempio, fornire tra le tante possibilità la seguente "N69UèAsL".

Accanto a questa tecnica, per ottenere password ancora più "forti", si possono sostituire le lettere risultanti dalla compressione della frase, con cifre o caratteri che assomiglino alle lettere; ad esempio la frase "Questo può essere un modo per ricordare la password" diventa "Qp&1mpRP".

Un altro modo per ottenere password "forti" consiste nel combinare date o numeri che si ricordano facilmente con pezzi di parole che sono in qualche modo abituali e quindi semplici da ricordare; ad esempio la combinazione "felice1983", che utilizzata direttamente potrebbe essere una password "debole" (combinazione del nome del figlio e della data di nascita), può diventare una password migliore in questo modo "FeLi83ce", o una password "forte" così "F&Li83cE".

N.B. Non utilizzare come password gli esempi riportati nelle presenti regole.

Sezione E Interventi formativi ed altre incombenze

Punto 1) Natura e pianificazione degli interventi formativi (regola 19.6, all. B D.Lgs. 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

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

Allo stato attuale non vi sono in corso contratti di affidamento di trattamento dati all'esterno della struttura, ad eccezione di quanto previsto nel contratto con Axios Italia s.r.l. per l'applicativo di Segreteria Digitale.

Si trasmettono dati inoltre 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 dei dati identificativi (regola 19.8, all. B D.Lgs. 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, fornitori e dipendenti ancorché disponibili nei fascicoli degli stessi. 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.Lgs. 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.Lgs.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.Lgs. 196/2003.

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

Baranzate, 4 gennaio 2022

Il titolare dei trattamenti Il Dirigente Scolastico dott. Marco Paolo Morini