

Allegato: “Misure di sicurezza” e di “garanzia” di cui all’articolo 32 e ss. del GDPR e all’art. 2 septies del D. Lgs. 101/18

- SCOPO
- LE DIMENSIONI DELLE ANALISI
- MISURE DI SICUREZZA FISICHE
- MISURE DI SICUREZZA LOGICHE
- MISURE DI SICUREZZA ORGANIZZATIVE

SCOPO

In questa sezione sono riportate, in forma sintetica e schematica, le misure in essere e da adottare per contrastare i rischi individuati. Per misura si intende lo specifico intervento tecnico od organizzativo posto in essere per prevenire, contrastare o ridurre gli effetti relativi ad una specifica minaccia, come pure quelle attività di verifica e controllo nel tempo, essenziali per assicurarne l'efficacia.

Secondo la definizione ISO, la sicurezza è “l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite” e dunque l'insieme di tutte le misure atte a difendere il sistema informatico dalle possibili minacce d'attacco.

Rendere sicuro un sistema informatico non significa esclusivamente attivare un insieme di contromisure specifiche, di carattere tecnologico ed organizzativo, che neutralizzino tutti gli attacchi ipotizzabili al sistema di servizi, ma significa, in particolare, collocare ciascuna delle contromisure individuate in una politica organica di sicurezza, che tenga conto dei vincoli (tecnici, logistici, organizzativi, amministrativi e legislativi) imposti dalla struttura tecnica ed organizzativa, in cui il sistema di servizi opera e che giustifichi ciascuna contromisura in un quadro complessivo.

Principale obiettivo di un sistema di sicurezza è la salvaguardia delle informazioni.

*Si individuano **tre** aspetti fondamentali relativi alla sicurezza delle informazioni:*

- **Confidenzialità:** solo gli utenti autorizzati possono accedere alle informazioni necessarie;
- **Integrità:** protezione contro alterazioni o danneggiamenti, tutela dell'accuratezza e completezza dei dati;
- **Disponibilità:** le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

L'approccio alla sicurezza deve avvenire in una logica di prevenzione (risk assessment) piuttosto che in una logica di gestione delle emergenze o di semplice controllo/vigilanza.

L'architettura per rispondere alle esigenze di sicurezza è costituita da 3 elementi fondamentali:

- a) le politiche dell'organizzazione;*
- b) gli strumenti organizzativi e tecnologici;*
- c) gli atteggiamenti individuali.*

Un sistema di gestione della sicurezza delle informazioni efficiente ed efficace permette all'organizzazione di:

- a) mantenersi aggiornata su nuove minacce e vulnerabilità e prenderle in considerazione in modo sistematico;
- b) trattare incidenti e perdite in ottica di prevenzione e di miglioramento continuo del sistema;
- c) sapere quando politiche di sicurezza e procedure non sono implementate, in tempo utile per prevenire danni;
- d) implementare politiche e procedure di primaria importanza.

LE DIMENSIONI DELLE ANALISI

Le Misure di sicurezza che l'Istituto Comprensivo n.5 di Imola adotta sono state scelte con riferimento a criteri e procedure fisiche, logiche, organizzative e tecniche, in grado di assicurare:

- a) la protezione delle aree e dei locali in cui sono conservati i dati;
- b) il controllo sull'accesso nei predetti locali delle persone autorizzate;
- c) l'integrità dei dati;
- d) la trasmissione dei dati, ivi comprese le misure di sicurezza da adottarsi per le restrizioni di accesso per via telematica.

L'obiettivo è esplicitare lo stato dell'arte dell'Istituto Comprensivo n.5 di Imola in termini di copertura rispetto ai requisiti minimi ed idonei delle misure di sicurezza previste dalla Legge, come dettagliato nei paragrafi successivi.

MISURE DI SICUREZZA - ARCHIVI CARTACEI

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	Aver cura degli atti e dei documenti contenenti dati personali	C.	Tutti gli incaricati hanno ricevuto una formazione dedicata in materia di Protezione dei dati personali.
ADEGUATA	Procedere all'archiviazione dei dati dopo l'uso negli appositi spazi messi a disposizione dall'organizzazione	C.	Tutti gli incaricati hanno ricevuto una formazione dedicata in materia di Protezione dei dati personali.
ADEGUATA	Divieto di lasciar documenti incustoditi , anche per brevi periodi, trasmetterli o consegnarli a terzi senza preventiva specifica autorizzazione	C.	Tutti gli incaricati hanno ricevuto una formazione dedicata in materia di Protezione dei dati personali.
ADEGUATA	Divieto di divulgare all'esterno il contenuto degli stessi archivi.	C.	Tutti gli incaricati hanno ricevuto una formazione dedicata in materia di Protezione dei dati personali.
ADEGUATA	Identificare e registrare le persone ammesse a qualunque titolo dopo gli orari di chiusura degli uffici.	C.	Nessuno è autorizzato ad entrare nell'Istituto dopo l'orario di chiusura.

MISURE DI SICUREZZA FISICHE

<i>TIPO</i>	<i>MISURE DI SICUREZZA</i>	<i>STATO</i>	<i>RACCOMANDAZIONI e NOTE</i>
<i>ADEGUATA</i>	<i>Accesso selezionato e controllato.</i>	<i>C.</i>	<i>La porta di accesso è gestita attraverso un ingresso controllato da un front office dedicato.</i>
<i>ADEGUATA</i>	<i>Definizione e delimitazione di aree di sicurezza.</i>	<i>C.</i>	<i>Presenza del personale dipendente.</i>
<i>ADEGUATA</i>	<i>Messa in sicurezza delle attrezzature decentralizzate per il trattamento dei dati personali, tra cui anche personal computer, laptop, tablet, smartphone, etc.</i>	<i>C.</i>	<i>Tutti i dispositivi vengono riposti in appositi armadi a fine giornata.</i>
<i>ADEGUATA</i>	<i>Registrazione, monitoraggio, e tracciamento degli accessi al data center dove sono conservati i dati personali.</i>	<i>C.</i>	<i>Firewall presente.</i>
<i>ADEGUATA</i>	<i>Vigilanza esterna.</i>	<i>N.P.</i>	<i>Non è presente una società di vigilanza esterna</i>
<i>ADEGUATA</i>	<i>Dispositivi di allarme.</i>	<i>P.</i>	<i>Attivazione e disattivazione manuale. Presente impianto di allarme con collegamento esterno.</i>
<i>ADEGUATA</i>	<i>BACK-UP (almeno settimanale) dei Dati.</i>	<i>C.</i>	<i>Il back-up avviene giornalmente in maniera automatica: - su ogni server (compreso il gestionale); - Fisico due NAS.</i>
<i>ADEGUATA</i>	<i>Conservare i BACK-UP in un luogo sicuro (in un contenitore ignifugo) o in Cloud</i>	<i>C.</i>	<i>Il Back up viene conservato: - Tramite due NAS custodito in armadio Rack</i>
<i>ADEGUATA</i>	<i>Verificare i BACK-UP almeno ogni 15 giorni per il controllo di integrità e leggibilità dei supporti</i>	<i>C.</i>	<i>I Back up vengono controllati attraverso regolari operazioni di ripristino.</i>
<i>ADEGUATA</i>	<i>Sala server con adeguate condizioni di uso e di archivio</i>	<i>N.C.</i>	<i>La sala server nell'ufficio del DSGA. E' presente un impianto di condizionamento. Armadio Rack non presente per server ma solo per dischi di back-up</i>
<i>ADEGUATA</i>	<i>Conservazione dei documenti cartacei.</i>	<i>C.</i>	<i>Tutti i documenti cartacei vengono conservati in armadi appositi chiusi a chiave, o ubicati in stanze chiuse a chiave, o inseriti in cassaforte; Fascicolo cartaceo: ufficio</i>

IC n.5 di Imola	ALLEGATO: MISURE DI SICUREZZA
------------------------	--------------------------------------

			<i>amministrativo, chiuso con chiave. Archivio storico: in stanza chiusa a chiave.</i>
<i>ADEGUATA</i>	<i>Chiavi di accesso</i>	<i>C.</i>	<i>Le chiavi di accesso sono consegnate al personale incaricato.</i>
<i>ADEGUATA</i>	<i>Sistema antincendio.</i>	<i>P.</i>	
<i>ADEGUATA</i>	<i>Gruppo di continuità elettrica.</i>	<i>P.</i>	<i>Presente.</i>

GESTIONE DELLE UTENZE E CONTROLLO DEGLI ACCESSI AI SISTEMI DI TRATTAMENTO DEI DATI PERSONALI

<i>TIPO</i>	<i>MISURE DI SICUREZZA</i>	<i>STATO</i>	<i>RACCOMANDAZIONI e NOTE</i>
<i>ADEGUATA</i>	<i>Identificazione del terminale e/o dell'utente che accede ai sistemi.</i>	<i>C.</i>	<i>Tramite credenziali</i>
<i>ADEGUATA</i>	<i>Sospensione automatica del terminale lasciato inattivo, con la necessità di inserire identificazione utente e password per riavviarlo</i>	<i>C./N.C.</i>	<i>Sospensione da implementare.</i>
<i>ADEGUATA</i>	<i>Definizione, per ciascun utente, di un profilo di accesso ai dati personali adeguato al ruolo a questi assegnato e limitatamente ai soli diritti necessari per le fasi dell'elaborazione</i>	<i>C.</i>	<i>Tramite Mansionario</i>
<i>ADEGUATA</i>	<i>Registrazione, monitoraggio e tracciamento degli accessi eseguiti sul contenuto dei dati, con possibilità di ricostruire a ritroso la storia degli eventi</i>	<i>N.C.</i>	<i>Firewall non implementato o non presente in tutti i plessi.</i>

CONTROLLO DEGLI ACCESSI

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	Definire e pubblicare regole per la gestione delle utenze e dei profili di accesso e operativi	N.C. Parziale	All'interno della Nomina ad incaricato del Trattamento e Pubblicare le Politiche del DPO sul sito
ADEGUATA	Fornire precise istruzioni ai propri dipendenti e collaboratori sulle modalità con cui i dati personali del Titolare dovranno essere trattati	C.	Tutti gli incaricati hanno ricevuto una formazione dedicata in materia di Protezione dei dati personali.
ADEGUATA	Assegnare singoli terminali e/o utenze nominali, prevedendo deroghe solo ove strettamente necessario e limitatamente a specifiche funzioni	C.	Tramite tenuta registro.
ADEGUATA	Monitorare i soggetti autorizzati a cancellare e/o modificare i dati personali	C.	Tramite mansionario
ADEGUATA	Controllare periodicamente gli archivi, procedendo alla distruzione dei dati non più necessari e/o dei dati per i quali risulta terminato il periodo di conservazione indicato dal TITOLARE, in modo controllato e documentato	C./N.C.	Procedura da implementare.
ADEGUATA	Definire le policy e pubblicare le regole per la conservazione delle copie di backup, coerentemente con il periodo di conservazione indicato dal TITOLARE.	C./N.C.	Policy da Richiedere al Tecnico informatico interno.

MISURE DI SICUREZZA LOGICHE

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	Codice identificativo associato ad una Password per l'accesso ai PC.	C.	
ADEGUATA	Password di almeno 8 caratteri alfanumerici.	C.	Tutti i computer utilizzati possiedono una password conforme. Il Login viene dato all'atto dell'assunzione.
ADEGUATA	Profilazione - Codice identificativo associato ad una PSW per l'accesso alla segreteria digitale e al registro elettronico.	C.	Ogni dipendente ha un proprio login di accesso personalizzato.
ADEGUATA	Utilizzo di programmi ANTIVIRUS.	C.	È presente un Antivirus che viene aggiornato in automatico è presente sul Cloud (WorryFree). Nei pc della didattica presente antivirus license free.
ADEGUATA	Utilizzo di programmi FIREWALL.	N.C. parziale	Presente Firewall nella scuola primaria, secondaria e AULA 3.0. Uffici amministrativi sprovvisti
ADEGUATA	Divieto di utilizzo di Software non approvato.	N.P.	Divieto da implementare.
ADEGUATA	Installazione di solo SOFTWARE licenziato.	C.	Mediasoft, Sidi e Msw
ADEGUATA	Controlli sul tipo di SOFTWARE installato al fine di rilevare quelli non appropriati.	P.	Autorizzazioni e controlli effettuati dal tecnico informatico.

MISURE DI SICUREZZA ORGANIZZATIVE

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	Periodica modifica dei Codici identificativi associati ad una PSW per l'accesso ai PC.	C.	Le password sono modificate almeno ogni 6 mesi
ADEGUATA	E' prevista la pseudonimizzazione e la cifratura dei dati personali?	N.C.	Si stanno implementando le procedure di pseudonimizzazione e di cifratura attraverso programmi appositi (es. Firma digitale).
ADEGUATA	E' prevista la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento?	C.	Vedi allegato misure di sicurezza ex. Art. 32 e ss. del GDPR. In particolare: - Relazione del DPO.
ADEGUATA	E' prevista la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico?	C.	In loco sono presenti due dispositivi NAS con funzione di Back up, oltre al salvataggio dei dati da parte del server. Vedi la politica allegata al MSG (Manuale di Sistema di Gestione privacy) – Incidenti: dall'incidente al post-risoluzione.
ADEGUATA	Disattivazione del codice (e di eventuali altre password e credenziali) in caso di cambiamento/termine della mansione.	N.C. parziale	Avviene a carico del Personale incaricato a fine anno scolastico. Gestito manualmente.
ADEGUATA	È prevista una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento?	C.	Vulnerability Assessment , effettuato ogni 30 gg.
ADEGUATA	Aggiornamento programma ANTIVIRUS.	C.	Centralizzato ed Automatico.
ADEGUATA		C.	Firewall presente.

IC n.5 di Imola	ALLEGATO: MISURE DI SICUREZZA
------------------------	--------------------------------------

	<i>Aggiornamento programma FIREWALL.</i>		
<i>ADEGUATA</i>	<i>Divieto di utilizzo di Software non approvato.</i>	<i>N.P.</i>	<i>Pur non essendo presente una procedura apposita, non sono comunque stati rilevati software senza licenza sui computer.</i>
<i>ADEGUATA</i>	<i>Installazione di solo SOFTWARE licenziato.</i>	<i>N.C.</i>	<i>L'utente è amministratore di Macchina, quindi può installare qualsiasi software.</i>
<i>ADEGUATA</i>	<i>Controlli sul tipo di SOFTWARE installato (download) al fine di rilevare quelli non appropriati.</i>	<i>C.</i>	<i>Effettuati dal tecnico informatico ogni mese.</i>
<i>ADEGUATA</i>	<i>Divieto di accesso a siti Internet non autorizzati.</i>	<i>C.</i>	<i>Black/white List implementata.</i>
<i>ADEGUATA</i>	<i>La società possiede un sito Web con dominio personale?</i>	<i>C.</i>	<i>-</i>
<i>ADEGUATA</i>	<i>È stata predisposta l'informativa sul Sito Web tramite link apposito?</i>	<i>C</i>	<i>Presente</i>
<i>ADEGUATA</i>	<i>Sono stati predisposti i moduli di consenso al Trattamento all'interno del sito Web aziendale, ad esempio per i servizi di newsletter?</i>	<i>C.</i>	<i>Presenti</i>
<i>ADEGUATA</i>	<i>Sono stati predisposti i cookies obbligatori per il sito web?</i>	<i>C.</i>	<i>Presenti.</i>

LEGENDA:

C.: Conforme N.C.: Non conforme (ADEGUATEZZA OBBLIGATORIA)

N.P.: Non presente P.: Presente (ADEGUATEZZA SUFFICIENTE)

Verona (VR), 11/03/2020

IC n.5 di Imola – Titolare del Trattamento

ANALISI DEI RISCHI CHE INCOMBONO SUI DATI

MISURE IN ESSERE E DA ADOTTARE PER GARANTIRE L'INTEGRITA' E LA DISPONIBILITA' DEI DATI

*Alla luce dei fattori di rischio individuati nel precedente paragrafo, vengono **descritte** di seguito le misure atte a garantire:*

- **la protezione delle aree e dei locali** ove si svolge il trattamento dei dati personali;
- **la corretta archiviazione** e custodia di atti, documenti e supporti contenenti dati personali;
- **la sicurezza logica**, nell'ambito degli strumenti elettronici.

La presente analisi prende in considerazione sia le misure già adottate al momento della stesura del presente Sistema privacy, sia le ulteriori misure finalizzate ad incrementare il livello di sicurezza nel trattamento dei dati.

PROTEZIONE DI AREE E LOCALI

Vengono di seguito analizzate le misure di sicurezza adottate e da adottare dall'Istituto Comprensivo n.5 di Imola in riferimento alla protezione di aree e locali in cui avvengono i trattamenti dei dati.

- **Struttura fisica della sede e dei plessi.** *L'edificio presso cui è ubicata la sede dell'Istituto Comprensivo n.5 di Imola risulta relativamente recente nella tipologia di costruzione. Tutti gli edifici risultano strutturalmente sani e idonei all'uso, non appare ipotizzabile un improvviso collasso strutturale considerato che non vi sono segni di degrado evidenti.*
- **Protezione dall'accesso esterno.** *L'edificio dell'Istituto Comprensivo n.5 di Imola è dotato di portone di ingresso tradizionale ad apertura controllata. Durante l'orario di lavoro l'accesso è controllato dal personale. Ogni finestra è dotata di persiane/infissi che vengono chiusi dopo l'orario di lavoro. I vetri sono a norma di legge. Gli edifici sono dotati di impianto di allarme esterno perimetrale, così come risultano allarmate i locali dove sono presenti i computer in uso presso gli uffici. Non si ritiene opportuno adottare ulteriori misure fisiche di sicurezza per scongiurare l'ingresso nel palazzo da parte di estranei.*
- **Accesso ai singoli locali:** *in generale, la sorveglianza dei singoli locali, che custodiscono archivi informatici ed elettronici, durante l'orario di lavoro è garantita dalla presenza del personale incaricato. In caso di temporanee assenze durante l'orario di lavoro, non vi è il pericolo che soggetti interessati ai servizi entrino nei locali della struttura con la possibilità di accesso non consentito ai dati ivi custoditi. Si è deciso comunque di adottare le seguenti misure di sicurezza adeguate a scongiurare tutti i tipi di rischio collegato:*

1. **Adozione di serrature** in tutte le porte dei singoli uffici.

2. **Definizione degli incaricati** preposti ad accedere ai singoli locali e fornitura delle chiavi dei rispettivi locali.

3. **Definizione delle istruzioni** da seguire da parte degli incaricati circa la chiusura dei singoli locali durante la loro assenza.

4. Sono state inserite nelle lettere d'incarico degli incaricati e dei Responsabili alcune norme comportamentali che disciplinino l'uso delle chiavi dei locali (vedi lettere d'incarico). In generale, comunque, le istruzioni prevedono che ogni incaricato sia in possesso di copia delle chiavi dell'ufficio/struttura in cui opera. All'inizio della giornata lavorativa come regola il primo incaricato che arriva nel proprio ufficio apre la porta con la chiave e disattiva l'allarme, e l'ultimo che lo lascia la richiude a chiave immettendo l'allarme tramite codice digitale. Ogni incaricato ha la custodia delle proprie chiavi.

· **Accesso ai locali fuori dall'orario di lavoro.** Nessuno accede ai locali dell'Istituto Comprensivo n.5 di Imola fuori dall'orario di lavoro.

· **Altre misure di sicurezza** finalizzate ad evitare l'accesso da parte di estranei. Al fine di incrementare la sicurezza contro l'accesso di estranei fuori dall'orario di lavoro, il Titolare ha installato un impianto di allarme, dando ad ogni incaricato e/o responsabile del trattamento un codice di attivazione e disattivazione personale. L'impianto è collegato alla vigilanza.

· **Rischi idrogeologici.** Per ciò che concerne il rischio di perdita dei dati in seguito ad allagamento, considerata la posizione dell'immobile in cui è situato l'edificio, si esclude che detto rischio possa verificarsi.

· **Rischi sismici.** La zona non è considerata a rischio di movimenti tellurici.

· **Protezioni antincendio.** In riferimento al rischio di incendio, gli impianti degli immobili con funzione di prevenire, eliminare, limitare o segnalare incendi sono di realizzazione recente e viene effettuata comunque in maniera regolare la verifica periodica di caldaie, impianto elettrico, etc. I locali, a norma, sono comunque forniti di estintori, a norma del Testo Unico n. 81/2008 e/o di sistemi di spegnimento e idranti. Viene così scongiurato il pericolo di perdita dati in seguito ad incendio.

CUSTODIA E ARCHIVIAZIONE DEI DATI

Vengono di seguito analizzate le modalità di custodia ed archiviazione dei documenti cartacei con relative misure di sicurezza dell'Istituto Comprensivo n.5 di Imola.

- **Separazione** dei documenti. *Il Titolare ha distribuito i diversi documenti contenenti dati personali in vari armadi negli uffici amministrativi, in modo distinto per le diverse funzioni istituzionali.*
- **Conservazione** dei documenti. *I documenti contenenti “dati sensibili” sono conservati in vari armadi anche non chiusi a chiave. Poiché l'adozione di armadi chiudibili a chiave non viene ritenuta misura idonea a scongiurare il pericolo di accesso non autorizzato ai vari archivi, si è deciso di considerare come autonomi archivi i singoli locali. Questi, quindi, sono stati chiusi a chiave dai collaboratori scolastici alla fine della giornata lavorativa. È altresì presente una cassaforte, destinata a conservare i documenti più riservati.*
- **Utilizzazione** dei documenti. *I vari documenti vengono utilizzati per il tempo strettamente necessario allo svolgimento del singolo incarico e, nell'ipotesi di ricevimento di utenti, gli stessi vengono chiusi per evitare letture indesiderate dei dati contenuti ovvero la lettura a contrario dei documenti.*
- **Distruzione** dei documenti non necessari al trattamento. *L'Istituto Comprensivo n.5 di Imola è provvisto di una procedura interna ufficiale prima di poter distruggere qualsiasi documento. I documenti sono conservati per un tempo illimitato.*
- **Formazione** degli incaricati. *Al fine di eseguire in maniera corretta i singoli trattamenti e la custodia dei documenti contenenti i dati personali, il personale incaricato dovrà seguire i corsi di formazione come specificato nel sistema di gestione privacy. I corsi sono finalizzati a ridurre i rischi di errori umani nella gestione fisica e logica dei trattamenti.*

Imola (BO), 11/03/2020

IC n.5 di Imola – Titolare del Trattamento

Firma _____

IC n.5 di Imola	ALLEGATO: MISURE DI SICUREZZA
------------------------	--------------------------------------