

**Allegato “Misure di sicurezza” e di “Garanzia” di cui
all’articolo 32 e ss. del GDPR e all’art. 2 septies del D. Lgs. n.
196/03, così come modificato dal D. lgs. n. 101/18**

SCOPO

LE DIMENSIONI DELLE ANALISI

MISURE DI SICUREZZA – ARCHIVI CARTACEI

MISURE DI SICUREZZA - GESTIONE E CONTROLLO DEGLI ACCESSI AI SISTEMI

MISURE DI SICUREZZA LOGICHE – PROTEZIONE DATI INFORMATICI

MISURE DI SICUREZZA ORGANIZZATIVE

MISURE DI SICUREZZA per il SITO WEB

MISURE DI SICUREZZA FISICHE

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 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 in termini di copertura rispetto ai requisiti minimi ed idonei delle misure di sicurezza previste dalla Legge, come dettagliato nei paragrafi successivi.

IC GANDHI PC	6.4 ALLEGATO: MISURE DI SICUREZZA
---------------------	--

MISURE DI SICUREZZA - ARCHIVI CARTACEI

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

CONSERVAZIONE DEI DOCUMENTI

<i>ADEGUATA</i>	<i>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</i>	<i>C.</i>	
-----------------	---	-----------	--

IC GANDHI PC	6.4 ALLEGATO: MISURE DI SICUREZZA
---------------------	--

GESTIONE E CONTROLLO DEGLI ACCESSI AI SISTEMI (es. Softwarehouse)

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	Codice identificativo associato ad una Password per l'accesso ai PC.	C.	
ADEGUATA	Assegnare singoli terminali e/o utenze nominali, prevedendo deroghe solo ove strettamente necessario e limitatamente a specifiche funzioni	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	Periodica modifica dei Codici identificativi associati ad una PSW per l'accesso ai PC.	C.	Le password devono essere modificate almeno ogni 6 mesi (ogni 3 mesi in caso di trattamento di dati sensibili o particolari).
ADEGUATA	Profilazione - Codice identificativo associato ad una PSW per l'accesso al gestionale	C.	Ogni dipendente ha un proprio login di accesso personalizzato.
ADEGUATA	Definire e pubblicare <u>regole</u> per la gestione delle utenze e dei profili di accesso e operativi	C.	Regole disponibili tramite mansionario
ADEGUATA	Fornire precise istruzioni ai propri dipendenti e collaboratori sulle modalità con cui i dati personali del Titolare dovranno essere trattati	C.	Istruzioni disponibili nel Sistema di Gestione. Si raccomanda la pubblicazione mediante affissione delle politiche operative di gestione dei dati nei locali di segreteria.
ADEGUATA	Identificazione del terminale e/o dell'utente che accede ai sistemi.	C.	Profilazione e credenziali di accesso univoche
ADEGUATA	Sospensione automatica del terminale lasciato inattivo, con la necessità di inserire identificazione utente e password per riavviarlo	C.	Misura implementata
ADEGUATA	Blocco automatico dell'identificazione utente in caso di errato inserimento della password e/o dell'utenza e tracciamento dei tentativi di accesso effettuati	C.	Misura implementata
ADEGUATA	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	C.	Credenziali di accesso univoche

IC GANDHI PC	6.4 ALLEGATO: MISURE DI SICUREZZA
---------------------	--

MISURE DI SICUREZZA LOGICHE – PROTEZIONE DATI INFORMATICI

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	Utilizzo di programmi ANTIVIRUS .	C.	Antivirus Windows Defender gratuito anche sui PC di segreteria
ADEGUATA	Aggiornamento programma ANTIVIRUS .	C.	
ADEGUATA	Sistemi operativi aggiornati nei PC in uso.	C.	Sono presenti PC con S.O. aggiornati
ADEGUATA	Utilizzo di programmi FIREWALL .	C.	Zyxel ATP700. Il Firewall viene aggiornato in automatico.
ADEGUATA	Aggiornamento programma FIREWALL .	C.	Firewall con hardware dedicato.
ADEGUATA	Registrazione, monitoraggio, e tracciamento degli accessi al data center dove sono conservati i dati personali.	C.	Tramite firewall.
ADEGUATA	Divieto di accesso a siti Internet non autorizzati. (Filtri siti web)	C.	Tramite firewall.
ADEGUATA	Monitorare i soggetti autorizzati a cancellare e/o modificare i dati personali	C.	
ADEGUATA	BACK-UP (almeno settimanale) dei Dati.	N.C.	
ADEGUATA	Conservare i BACK-UP in un luogo sicuro (in un contenitore ignifugo) o in Cloud	N.C.	
ADEGUATA	Verificare i BACK-UP almeno ogni 15 giorni per il controllo di integrità e leggibilità dei supporti		
ADEGUATA	Sala server con adeguate condizioni di uso e di archivio	N.C.	Il server è posto nell'ufficio DSGA, l'accesso è libero. Il Firewall è posizionato nell'armadio rack di segreteria
ADEGUATA	Gruppo di continuità elettrica .	P.	

MISURE DI SICUREZZA ORGANIZZATIVE

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	È prevista la pseudonimizzazione/ anonimizzazione e la cifratura dei dati personali?	N.C.	Si stanno implementando le procedure di pseudonimizzazione e di cifratura attraverso programmi appositi (es. PEI; PDP, Allegati e-mail, Sito web HTTPS,).
ADEGUATA	È 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	È prevista la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico?	C.	In loco è presente un dispositivo 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.	C.	Avviene a carico del Personale incaricato.
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?	N.C.	Si consiglia di prevedere con il consulente informatico un esame di Vulnerability Assessment , (da implementare) a cadenza ciclica.
ADEGUATA	Divieto di utilizzo di Software non approvato.	N.P.	Utente hanno poteri illimitati
ADEGUATA	Controlli sul tipo di SOFTWARE installato al fine di rilevare quelli non appropriati.	N.P.	Non sono presenti controlli sul tipo di software installato
ADEGUATA	Installazione di solo SOFTWARE licenziato.	C.	SPAGGIARI
ADEGUATA	Piattaforme in uso	C.	GOOGLE WORKSPACE FOR EDU

IC GANDHI PC	6.4 ALLEGATO: MISURE DI SICUREZZA
---------------------	--

MISURE DI SICUREZZA per il SITO WEB

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	L'Istituzione possiede un sito Web con dominio personale?	C.	https://www.icsannicolo.edu.it/
ADEGUATA	E' stata effettuata la nomina come Responsabile esterno del trattamento alla società esterna che gestisce il sito?	C.	Infocima
ADEGUATA	È stata predisposta l' informativa (facendo riferimento eventualmente anche all'area riservata) sul Sito Web tramite link apposito?	C.	Presente
ADEGUATA	È stato raccolto il consenso dagli interessati qualora nel Sito Web fossero pubblicati foto/audio/video?	C.	Ottenuto ad inizio del ciclo scolastico
ADEGUATA	Sono state predisposte le 3 informative privacy (alunni/famiglie, dip.e fornitori) nella sez. privacy?	C.	Presenti
ADEGUATA	Il DPO è stato pubblicizzato nella sez. privacy?	C.	Dati presenti e aggiornati
ADEGUATA	È presente un Cookie banner con flag di spunta per eventuali cookie analitici e/o di profilazione? È presente una Cookie policy?	C.	Cookie banner e cookie policy presenti
ADEGUATA	È presente la dichiarazione di accessibilità al sito web secondo indicazioni AgID?	C.	Dichiarazione di accessibilità: presente
ADEGUATA	Sono stati pubblicati gli Obiettivi di accessibilità?	C.	Presenti 2023
ADEGUATA	È stato pubblicato in Amministrazione trasparente il Manuale di gestione dei flussi documentali con i relativi allegati?	P.	

MISURE DI SICUREZZA FISICHE

TIPO	MISURE DI SICUREZZA	STATO	RACCOMANDAZIONI e NOTE
ADEGUATA	Accesso selezionato e controllato.	C.	La porta di accesso è gestita attraverso un ingresso controllato da un front office dedicato.
ADEGUATA	Definizione e delimitazione di aree di sicurezza.	C.	DVR presente
ADEGUATA	Messa in sicurezza delle attrezzature decentralizzate per	C.	

IC GANDHI PC	6.4 ALLEGATO: MISURE DI SICUREZZA
---------------------	--

	<i>il trattamento dei dati personali, tra cui anche personal computer, laptop, tablet, smartphone, etc.</i>		
<i>ADEGUATA</i>	<i>Vigilanza esterna.</i>	<i>N.P.</i>	
<i>ADEGUATA</i>	<i>Impianto di videosorveglianza</i>	<i>N.P.</i>	
<i>ADEGUATA</i>	<i>Dispositivi di allarme.</i>	<i>P. parziale</i>	<i>Attivazione e disattivazione manuale. Presente impianto di allarme con collegamento esterno solo in alcuni plessi.</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>	

LEGENDA:

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

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

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 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 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 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.*
- *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 esterni del*

*trattamento dei dati personali 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.*

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

· ***Altre misure di sicurezza finalizzate ad evitare l'accesso da parte di estranei.***

· ***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.

· **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 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 dal personale 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 è provvisto di una procedura interna ufficiale tramite trita documenti per 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.*

Rottofreno (PC), 28/07/2023

Istituto Comprensivo "Gandhi" (San Nicolò) – Titolare del Trattamento

Firma 

