Allegato: "Misure di sicurezza" e di "garanzia" di cui all'articolo 32 e ss. del GDPR e all'art. 7 septies del D. Lgs. 101/18

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 Castello di Serravalle - Savigno 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 Castello di Serravalle - Savigno 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

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.*	
ADEGUATA	*Messa in sicurezza delle attrezzature decentralizzate per il trattamento dei dati personali, tra cui anche personal computer, laptop, tablet, smartphone, etc.*	*C.*	*Dispositivi riposti in un armadio dedicato a fine giornata lavorativa (Da verificare in Fase di Revisione con il DPO).*
ADEGUATA	*Registrazione, monitoraggio, e tracciamento degli accessi al data center dove sono conservati i dati personali.*	*N.C.*	*Firewall non presente.*
ADEGUATA	*Vigilanza esterna.*	*N.P.*	*Non è presente una società di vigilanza esterna.*
ADEGUATA	*Dispositivi di allarme.*	*P.*	*E' presente un impianto di allarme solo in alcuni plessi.*
ADEGUATA	*BACK-UP (almeno settimanale) dei Dati.*	*C.*	*Il back-up avviene giornalmente in maniera automatica:* *- su ogni server (compreso il gestionale);* *- Fisico su HD esterno. (Da verificare in Fase di Revisione con il DPO).*
ADEGUATA	*Conservare i BACK-UP in un luogo sicuro (in un contenitore ignifugo) o in Cloud*	*C.*	*Il Back up viene conservato:* - *Tramite HD esterno* - *Tramite una copia su Server*
ADEGUATA	*Verificare i BACK-UP almeno ogni 15 giorni per il controllo di integrità e leggibilità dei supporti*	*N.C.*	*I Back up non vengono controllati regolarmente.*
ADEGUATA	*Sala server con adeguate condizioni di uso e di archivio*	*C.*	*Il Server si trova in un locale con accesso limitato ed il locale è climatizzato.*

ADEGUATA	*Conservazione dei documenti cartacei.*	*C.*	*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: nel seminterrato, in stanza chiusa a chiave.*
ADEGUATA	*Chiavi di accesso*	*C.*	*Le chiavi di accesso sono consegnate al personale incaricato.*
ADEGUATA	*Sistema antincendio.*	*P.*	
ADEGUATA	*Gruppo di continuità elettrica.*	*P.*	

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

TIPO	*MISURE DI SICUREZZA*	*STATO*	*RACCOMANDAZIONI e NOTE*
ADEGUATA	*Identificazione del terminale e/o dell'utente che accede ai sistemi.*	*N.C.*	*Non è presente un sistema di identificazione dell'IP (Da verificare in Fase di Revisione con il DPO).*
ADEGUATA	*Sospensione automatica del terminale lasciato inattivo, con la necessità di inserire identificazione utente e password per riavviarlo*	*C.*	*Presente (Da verificare in Fase di Revisione con il DPO).*
ADEGUATA	*Blocco automatico dell'identificazione utente in caso di errato inserimento della password e/o dell'utenza e tracciamento dei tentativi di accesso effettuati*	*N.C.*	*Procedura da implementare dall'Amministratore di Sistema (Da verificare in Fase di Revisione con il DPO).*
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.*	*Tutti gli incaricati hanno ricevuto una* ***formazione*** *dedicata in materia di Protezione dei dati personali.*
ADEGUATA	*Registrazione, monitoraggio e tracciamento degli accessi eseguiti sul contenuto dei dati, con possibilità di ricostruire a ritroso la storia degli eventi*	*N.C.*	*Firewall non presente.*

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*	*C.*	*Tutti gli incaricati hanno ricevuto una **formazione** dedicata in materia di Protezione dei dati personali.*
ADEGUATA	*Fornire precise **istruzioni** ai propri dipendenti e collaboratori sulle modalità con cui i dati personali del Titolare dovranno essere trattati*	*C.*	*Tramite lettera presa d'incarico.*
ADEGUATA	*Assegnare singoli terminali e/o utenze nominali, prevedendo deroghe solo ove strettamente necessario e limitatamente a specifiche funzioni*	*N.C.*	*Non si dispone di assegnazioni utenze nominali ai singoli terminali*
ADEGUATA	***Monitorare** i soggetti autorizzati a cancellare e/o modificare i dati personali*	*C.*	
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.*	*(Da verificare in Fase di Revisione con il DPO).*
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.*	*(Da verificare in Fase di Revisione con il DPO).*

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.*	*Tutti gli incaricati sono provvisti di un identificativo per accedere al sistema.*
ADEGUATA	*Password di almeno 8 caratteri alfanumerici.*	*C.*	*Tutti i computer utilizzati possiedono una password conforme. Il Login aziendale 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.*	*N.C.*	*È presente un Antivirus (Open Source) che viene aggiornato in automatico. Posizione: presente su Server e su ogni PC in uso al personale.*
ADEGUATA	*Utilizzo di programmi FIREWALL.*	*N.C.*	*Il Firewall non è Presente.*
ADEGUATA	*Divieto di utilizzo di Software non approvato.*	*N.P.*	*Presente solo per i terminali in uso alla didattica. Pc della segreteria non richiedono autorizzazioni e sono liberi.*
ADEGUATA	*Installazione di solo SOFTWARE licenziato.*	*C.*	*Nuvola (Segreteria Digitale e Registro Elettronico), Mediasoft, Sidi e Sissi.*
ADEGUATA	*Controlli sul tipo di SOFTWARE installato al fine di rilevare quelli non appropriati.*	*N.P.*	*Non sono effettuati controlli regolari sui tipi di software installati*

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 devono essere modificate almeno ogni 6 mesi (ogni 3 mesi in caso di trattamento di dati sensibili o particolari).*
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 è presente un HD esterno con funzione di Back up, oltre al salvataggio dei dati da parte del server. (Da verificare in Fase di Revisione con il DPO).* *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.*	*La procedura viene effettuata dall'Amministratore di Sistema.*
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	*Aggiornamento programma ANTIVIRUS.*	*C.*	*Centralizzato ed Automatico.*

ADEGUATA	*Aggiornamento programma FIREWALL.*	*N.C.*	*Firewall non presente*
ADEGUATA	*Divieto di utilizzo di Software non approvato.*	*N.P.*	*Firewall non presente*
ADEGUATA	*Installazione di solo SOFTWARE licenziato.*	*C.*	
ADEGUATA	*Controlli sul tipo di SOFTWARE installato (download) al fine di rilevare quelli non appropriati.*	*C.*	*Vengono effettuati dei Controlli al fine di rilevare quelli non appropriati. (Da verificare in fase di Revisione con il DPO)*
ADEGUATA	*Divieto di accesso a siti Internet non autorizzati.*	*N.C.*	*Black List non presente.*
ADEGUATA	*La società possiede un sito Web con dominio personale?*	C.	https://iccastellodiserravalle.edu.it/
ADEGUATA	*È stata predisposta l'informativa sul Sito Web tramite link apposito?*	*C.*	
ADEGUATA	*Sono stati predisposti i moduli di consenso al Trattamento all'interno del sito Web aziendale, ad esempio per i servizi di newsletter?*	*C.*	*Moduli Presenti.*
ADEGUATA	*Sono stati predisposti i cookies obbligatori per il sito web?*	*N.C. Parziale*	*Cookie policy presente ma non conforme.*

LEGENDA:
C.: Conforme N.C.: Non conforme (ADEGUATEZZA OBBLIGATORIA)
N.P.: Non presente P.: Presente (ADEGUATEZZA SUFFICIENTE)

Valsamoggia (BO), 05/03/2020

La direzione

_____

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 Castello di Serravalle - Savigno 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 Castello di Serravalle - Savigno 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 Castello di Serravalle - Savigno 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. 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 inserire 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. Ogni incaricato ha la custodia delle proprie chiavi.

· ***Accesso ai locali fuori dall'orario di lavoro****. Nessuno accede ai locali dell'Istituto Comprensivo Castello di Serravalle - Savigno e dei plessi fuori dall'orario di lavoro.*

· ***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 anti incendio****. 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 Castello di Serravalle - Savigno.

· ***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 Castello di Serravalle - Savigno 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.*

Valsamoggia (BO), 05/03/2020

IC Castello di Serravalle - Savigno *– Titolare del Trattamento*

Firma _____