Istituto Scolastico Comprensivo "Castel di Lama Capoluogo"
Via Roma n. 107 - CASTEL DI LAMA (A.P.)
Tel. 0736/81.32.25 –E-mail: apic820001@istruzione.it

Allegato 2

MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI
PIANO D'AZIONE
IC CASTEL DI LAMA 1

A. Valutazione dei rischi e misure di prevenzione e protezione

Nelle tabelle che seguono si riportano le fattispecie per cui sono evidenziate le vulnerabilità ed il livello di gravità che questi eventi comporterebbero.
Le vulnerabilità sono di 3 tipi: "NO", per nessuna, "Parziale" e "SI" per vulnerabilità accertata.
Il livello di gravità dell'evento è espresso in 3 gradi: basso, medio e alto.

Descrizione rischio	Vulnerabilità	Livello di gravità	Danni individuabili
Sottrazione di credenziali di autorizzazione	Parziale	ALTO	Accesso, sottrazione o divulgazione di dati
Carenza di consapevolezza, disattenzione o incuria	No	ALTO	Divulgazione, corruzione o distruzione di dati
Comportamenti sleali o fraudolenti	Parziale	ALTO	Accesso, sottrazione, divulgazione o distruzione di dati
Errore materiale	SI	BASSO	Corruzione o distruzione parziale di dati
Malfunzionamento, indisponibilità o degrado degli strumenti	SI	ALTO	Perdita di file, corruzione ed indisponibilità del
Azione di virus, worm e male-	Parziale	MEDIO	Perdita di file, corruzione ed indisponibilità del sistema
Spamming o tecniche di sabotaggio	Parziale	MEDIO	Perdita di file, corruzione ed indisponibilità del sistema
Accessi non autorizzati a locali/reparti ad accesso ristretto	No	ALTO	Accesso, sottrazione, divulgazione o distruzione di dati
Sottrazione di strumenti contenenti dati	No	ALTO	Accesso, divulgazione o distruzione di dati

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

B. Misure in essere e di cui si prevede l'adozione

Dopo aver analizzato e valutato i fattori di rischio, relativi alle aree e locali, all'integrità dei dati e alle trasmissioni, sono state individuate le misure di prevenzione e protezione più idonee a ridurre o eliminare il rischio stesso.
L'insieme delle misure preventive e protettive riportate nella tabella seguente, costituisce un programma di fondamentale importanza nell'ambito della politica per la Sicurezza, poiché fornisce una guida operativa, che permette di gestire la Sicurezza stessa con organicità e sistematicità.
Le misure sono individuate per tipologia che si presentano come:

1.Preventiva laddove si tende a prevenire l'evento dannoso;
2..Obbligatoria per le misure espressamente definite dalla normativa;
3. di contrasto per tutte le misure che inibiscono gli effetti dell'evento dannoso;
4. 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 laddove si ravvisino necessità di intervento o sopraggiunte non conformità.

Misure	Tipologia di misura	Rischi contrastati	Misure già in essere	Misure da adottare
Installazione e configurazione sistema operativo server e client che gestisca le procedure di autenticazione	Preventiva	Accessi indesiderati e non controllati	SI	Nessuna
Gestione Credenziali di autenticazione a livello di sistema operativo e di procedura gestionale preposta al trattamento	Preventiva	Accessi indesiderati e non controllati	Solo password a livello utente senza la gestione delle scadenza e della conformità	Gestione scadenza ed assegnazione credenziali mediante policy di dominio ed eliminazione utenti standard per le procedure gestionali
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	SI	Nessuna

Misure	Tipologia di misura	Rischi contrastati	Misure già in essere	Misure da adottare
Antivirus, antispam	Di contrasto	Danneggiamenti o distruzione di dati, indisponibilità dei sistemi	SI parziale	Verifica periodica della protezione
Firewall e proxy server	Di contrasto	Danneggiamenti, diffusione o distruzione di dati, indisponibilità dei sistemi	SI	Nessuna
Procedure di backup automatizzato	Preventiva	Danneggiamenti o distruzione di dati	Si	Disporre la delocalizzazione dei supporti HD rimovibili
Procedura per custodia ed uso supporti rimovibili	Contenimento degli effetti	Danneggiamenti o distruzione di dati	Custodia in cassaforte	Redazione ed applicazione della procedura
Procedure di restore e di disaster recovery	Contenimento degli effetti	Danneggiamenti o distruzione di dati	Restore manuale, senza test e procedura per i data base e i documenti in lavorazione	Procedura e test di restore del sistema
Organizzazione delle policy di dominio, gestione dei gruppi organizzativi	Preventiva	Accessi indesiderati e non controllati, danneggiamenti o distruzione	Configurazione delle policy e dei gruppi organizzativi	Nessuna

Misure	Tipologia di misura	Rischi contrastati	Misure già in essere	Misure da adottare
Gestione di un server di dominio aggiuntivo o in cluster	Contenimento degli effetti	Indisponibilità dei sistemi	Nessuna	Disponibilità pc aggiuntivo, installazione e configurazione
Attivazione servizi di auditing e monitoraggio	Preventiva	Non tracciabilità di accessi o attività non consentite o fraudolente	Nessuna	Attivazione servizi di auditing e monitoraggio
Procedura di distruzione dei supporti removibili non più in uso	Di contrasto	Diffusione non controllata di dati	SI	Nessuna
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	SI	Nessuna
Procedura di sospensione automatica delle sessioni	Preventiva	Accessi indesiderati e non controllati	Parzialmente	Attivazione procedura di sospensione automatica su tutti i PC

Misure	Tipologia di misura	Rischi contrastati	Misure già in essere	Misure da adottare
Verifica funzionale periodica della funzionalità dei sistemi	Preventiva	Indisponibilità dei sistemi e affidabilità dei dati	SI	Verifica funzionale periodica della funzionalità dei sistemi
Vigilanza attiva della sede	Di contrasto	Accessi indesiderati e non controllati	NO	Nessuna
Vigilanza passiva della sede	Di contrasto	Accessi indesiderati e non controllati	Si, antifurto ad attivazione manuale	Nessuna
Registrazione accessi	Preventiva	Accessi indesiderati e non controllati	Registro di visita per gli estranei all'amministrazione	Nessuna
Autenticazione accessi	Di contrasto	Accessi indesiderati e non controllati	SI	Nessuna
Custodia in classificatori ed armadi con chiusura	Preventiva	Accessi indesiderati e non controllati	SI	Nessuna
Deposito in cassaforte o armadi blindati e/o antifiamma	Preventiva	Danneggiamenti o distruzione di dati	SI, cassaforte	Nessuna

Misure	Tipologia di misura	Rischi contrastati	Misure già in essere	Misure da adottare
Dispositivi antincendio	Contenimento degli effetti	Danneggiamenti o distruzione di dati, indisponibilità dei sistemi	SI, estintori	Dotarsi di estintori CO_2 specifici per strumenti elettronici
Limitazione dell'accesso dei locali ove risiede il server	Preventiva	Accessi indesiderati e non controllati	SI	Nessuna
Assegnazione formale di responsabilità ed incarichi	Obbligatoria	Non applicabilità del sistema di sicurezza	In corso di assegnazione a tutto il personale	Nessuna
Certificazione delle attività di società esterne	Obbligatoria	Malfunzionamento o non applicabilità del sistema di sicurezza	SI	nessuna
Formazione per gestione dati con trattamento non informatizzato, finalizzata al controllo degli accessi, alla custodia e conservazione	Obbligatoria	Non applicabilità del sistema di sicurezza	SI	Ripetere la sessione

Misure	Tipologia di misura	Rischi contrastati	Misure già in essere	Misure da adottare
Consultazioni registrate dei dati	Preventiva	Non rintracciabilità degli accessi ai dati	SI	Nessuna
Procedure di restore e di disaster recovery	Contenimento degli effetti	Danneggiamenti o distruzione di dati	Restore automatico a norma dei dati ®	Nessuna
Adozione di un Manuale di gestione documentale	Obbligatoria	Malfunzionamento della gestione amministrativa	SI	In attesa di approvazione
Adozione del Manuale di conservazione sostitutiva	Obbligatoria	Rischio di perdita dei documenti	SI	In attesa di approvazione

C . Criteri e modalità di ripristino

Criteri e procedure per il salvataggio	Supporto magnetico/ottico e luogo di custodia delle copie	Procedura di ripristino e pianificazione
Procedura backup di con cadenza periodica impostata a parametro in giorni da ultimo salvataggio. Valore variabile impostato dall'utente sulla base di procedura scritta	Salvataggio in cartella del server	Restore dati, nessuna pianificazione o test di funzionamento
Procedura backup automatico con cadenza giornaliera.	Salvataggio in server	Restore dati come da contratto

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'IC Castel di Lama 1, la sua immagine, la produttività degli operatori e il rispetto degli obblighi di legge. Gli obiettivi che si vogliono conseguire sono di garantire, in accordo con le leggi e le regole interne:

a) per le risorse tecnologiche:

 la disponibilità del servizio in una forma adeguata, anche a fronte di eventi eccezionali, tramite la formulazione di appropriati piani di recupero delle funzionalità del sistema;

 la continuità del servizio a copertura delle esigenze operative della scuola.

b) per i dati:

 la riservatezza delle informazioni;

 l'integrità delle informazioni;

 la correttezza delle informazioni ritenute critiche per le eventuali conseguenze derivanti da una loro alterazione;

 la disponibilità delle informazioni e delle relative applicazioni.

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

 dispositivi tecnologici (computer, terminali, linee di comunicazione, ...) il cui danneggiamento fisico può comportare l'interruzione del corretto funzionamento e la conseguente sospensione del servizio;

 sistemi operativi o prodotti software la cui modifica, cancellazione o indisponibilità può comportare l'interruzione del funzionamento e la conseguente sospensione del servizio oppure può comportare la possibilità di accesso e manomissione di dati riservati da parte di personale non autorizzato;

 programmi applicativi la cui modifica o cancellazione può compromettere l'esercizio di alcune funzioni del sistema informativo o alterarne le corrette caratteristiche di funzionamento;

 dati per i quali si richiedono riservatezza, integrità e disponibilità.

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

Procedure di Disaster Recovery (c3, lettera b, art. 50 bis del CAD)

Per disaster recovery s'intende l'insieme di misure tecnologiche e organizzative dirette a ripristinare sistemi, dati e infrastrutture necessarie all'erogazione di servizi a fronte di gravi problemi. 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'IC Castel di Lama 1 poiché, in caso di guasti, manomissioni o furti assicura che esista una copia dei dati, garantendo, quindi, una ridondanza logico/ fisica di questi ultimi. L'Istituto utilizza sistemi differenti di backup:

1) sempre on-line modalità cloud per i trattamenti informatizzati attraverso gli applicativi in uso (Axios, Nuvola);
2) off- site.

Il backup on-site è effettuato sul server presente nell'ufficio di segreteria; l'esecuzione del backup è impostata in maniera automatica e svolta con una periodicità stabilita di una volta al giorno.