8.2.2 Protezione da virus informatici

Per evitare la distruzione o la perdita di dati a causa di virus informatici, il Responsabile, con la collaborazione dell'Amministratore del sistema, stabilisce quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Viene, inoltre, stabilito dal Responsabile la periodicità di aggiornamento di tali sistemi antivirus che è fissata in almeno ogni 4 mesi per ottenere un accettabile standard di sicurezza delle banche dati trattati.

Per tracciare l'eventuale introduzione di virus, l'Amministratore del sistema predisporrà un opportuno modulo di "Rilevazione di virus informatico" dove, su segnalazione degli incaricati, indicherà il sistema infettato, il tipo di virus e la fonte da cui sono pervenuti (se possibile) al fine d'isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche. Tali moduli saranno conservati dal Responsabile in luogo sicuro e copia controllata sarà anche in possesso dell'Amministratore del sistema.

In caso di rilevazione e/o perdita di dati o danni a causa d'infezioni o contagio da virus informatico di uno o più sistemi, l'Amministratore del sistema deve provvedere a:

1. isolare il sistema;
2. verificare se ci sono altri sistemi infettati con lo stesso virus;
3. identificare l'antivirus adatto e bonificare il sistema infetto;
4. installare l'antivirus adatto su tutti gli altri sistemi che ne sono sprovvisti;
5. compilare e gestire il modulo "Rilevazione virus informatico" come già descritto.

8.2.3 Indicazioni tecniche

In questo paragrafo sono date alcune semplici indicazioni di tipo tecnico che sarebbe opportuno adottare sui personal computer utilizzati nell'Istituzione Scolastica. Dovrebbe essere compito dell'Amministratore del sistema verificare e, eventualmente, attuare tali accorgimenti.

- **Impostazioni di Windows**
  Il primo, grande problema di sicurezza è rappresentato dal modo in cui è impostato il Sistema Operativo. Se, ad esempio, si usa Windows occorre utilizzare la funzione denominata "Windows Update" che serve per aggiornare quasi automaticamente il Sistema Operativo, scaricando dal sito Microsoft tutte le "patch" di sicurezza necessarie. Una "patch" è un piccolo file che serve per risolvere un problema software. Occorre eseguire la stessa azione per il "browser", ossia il programma che consente di navigare in Internet (ad esempio "Internet Explorer").
- **Password di screen saver**
  È un sistema di protezione quando ci si allontana dalla postazione lasciando il PC acceso. Occorre eseguire le seguenti istruzioni: Start – Impostazioni – Pannello di Controllo – Schermo; selezionare la scheda "Screen Saver" e, in questa, selezionare uno screen saver e poi l'opzione "Protezione"; cliccare su "Applica", inserire la password e cliccare su "OK".
- **Opzioni di sicurezza del browser**
  Impostare il livello di protezione durante la navigazione su livelli medio – alti (per es., con "Internet Explorer 6" Strumenti – Opzioni Internet – Protezione – Livello personalizzato – Impostazioni personalizzate e scegliere o media o alta). Con "Internet Explorer 6" si possono rifiutare anche i "cookies" (letteralmente "biscotti", altri programmi disturbatori) tramite Strumenti – Opzioni Internet – Privacy – protezione massima o quella immediatamente inferiore.
- **Password di apertura e scrittura di Word ed Excel**
  Quando si elabora un file con Word o Excel di Microsoft è possibile associare una password da digitare obbligatoriamente per poterlo leggere e/o modificare: File – Salva con nome – nella finestra che si apre selezionare Strumenti – Opzioni Generali – scrivere la password in una delle due caselle "password di apertura" e "password di modifica"; nel primo caso il documento non può essere aperto senza conoscere la password, nel secondo caso sarà visibile ma non modificabile.

8.3 MISURE DI SICUREZZA CONTRO IL RISCHIO DI ACCESSO NON AUTORIZZATO

8.3.1 Norme generali di prevenzione

In considerazione di quanto disposto dal D. Lgs 196/03 è fatto divieto a chiunque di:

1. effettuare copie di dati su supporti magnetici o trasmettere dati senza l'autorizzazione del Responsabile del trattamento;
2. effettuare copie fotostatiche o di qualsiasi altra natura, non autorizzate dal Responsabile, di stampe, tabulati, elenchi, rubriche e di ogni altro materiale riguardante i dati oggetto del trattamento;
3. sottrarre, cancellare, distruggere stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento senza l'autorizzazione del Responsabile;
4. consegnare a persone non autorizzate dal Responsabile stampe, tabulati, elenchi, rubriche e ogni altro materiale riguardante i dati oggetto del trattamento.

8.3.2 Procedure per controllare l'accesso ai locali in cui vengono trattati i dati

Il Responsabile deve definire le modalità di accesso agli uffici e/o agli archivi in cui sono presenti sistemi o apparecchiature di accesso ai dati. In particolare si dispone quanto segue:

1. gli originali di tutte le chiavi degli uffici e degli archivi cartacei, opportunamente identificate, sono conservate dal Responsabile in una cassetta chiusa in un luogo sicuro;
2. copie di tali chiavi sono consegnate agli incaricati preposti, registrando tale consegna in un apposito registro con controfirma di chi riceve tali copie;
3. l'accesso a tutte le aree ove vengono trattati i dati è consentito solo a personale autorizzato, per cui le porte di accesso devono essere normalmente chiuse e, in caso di allontanamento di tutti gli incaricati presenti in tale area, la porta deve essere chiusa a chiave;
4. su ogni porta di accesso alle aree di cui al punto 3 deve essere apposto un cartello che indichi che l'accesso è limitato al solo personale autorizzato;
5. agli utenti (alunni, genitori, fornitori, ecc.), se non espressamente autorizzati dal Responsabile, non è consentito l'accesso nelle aree di cui sopra; essi comunicano con gli Incaricati solo attraverso l'apposito sportello per il pubblico;
6. in caso di decadenza del compito di un incaricato, il Responsabile si farà riconsegnare le eventuali chiavi in dotazione del soggetto in questione e aggiornerà il registro in modo opportuno.

Qualora l'Istituzione Scolastica si dovesse avvalere per le pulizie, o per altri servizi, di imprese private e qualora i dipendenti di tali imprese, nell'ambito del servizio, avessero accesso ad aree contenenti archivi di dati personali, gli stessi dipendenti dovranno essere identificati e autorizzati dal Responsabile. Inoltre il servizio sarà effettuato sempre alla presenza di un Incaricato preposto a ciò e autorizzato dal Responsabile.

8.3.3 Procedure di assegnazione delle USER-ID

Il Responsabile, in collaborazione con l'Amministratore del sistema, deve definire le modalità di assegnazione dei nomi identificativi per consentire a ciascun Incaricato di accedere ai sistemi di trattamento delle banche dati. La user-id viene consegnata in busta chiusa al singolo incaricato e l'Amministratore del sistema avrà un registro, conservato in luogo sicuro, dove sono riportate le user-id emesse associate al singolo incaricato.

Non sono ammessi nomi identificativi di gruppo.

In ogni caso, un codice identificativo assegnato ad un Incaricato deve essere annullato se l'Incaricato decade dal suo compito. Il Responsabile comunicherà immediatamente l'evento all'Amministratore del sistema e al Custode delle credenziali che provvederanno a disattivare la possibilità di accesso al sistema per il soggetto in questione.

Nel caso specifico:

1. il DSGA li assegna per ARGO;
2. l'AT incaricato da amministratore di sistema l'assegna per l'accesso ai server e ai client;
3. il DS li assegna ai docenti e agli alunni o loro genitori per l'accesso a Scuolanet.

Da ognuno è tenuto opportuno registro che riporta le user id assegnate che va aggiornato ad ogni variazione.

8.3.4 Procedure di assegnazione delle PASSWORD

Il Responsabile, in collaborazione con l'Amministratore del sistema, assegna password provvisorie agli Incaricati i quali, al primo accesso, modificano autonomamente la propria password di accesso.

In particolare, vale lo stesso criterio di suddivisione riportato per le user id nel paragrafo precedente.

Tutti gli Incaricati devono cambiare le password ricevute e consegnarne copia scritta in busta chiusa e firmata al Custode delle credenziali che le conserverà in luogo sicuro. Tale busta sarà rinnovata ogni qualvolta l'incaricato la cambierà. **La password va cambiata almeno una volta ogni 3 mesi. I docenti che accedono a "Scuolanet" hanno l'obbligo di modificarla ogni 6 mesi in quanto, per questa applicazione, non sono trattati dati sensibili.**

Le password devono essere formate da almeno 8 caratteri, cifre e lettere, possibilmente maiuscole e minuscole (ad es. "sC52uOlA"). Sono da evitare:

- la ripetizione di due parole brevi anche rovesciate (ad es. "melapera" o "melaalem");
- le cifre all'inizio o in fondo alla password (ad es. "nicola57");
- riferimenti espliciti alla propria persona, famiglia o scuola;
- l'utilizzo della user-id o sequenze scontate e nomi comuni.

Gli incaricati devono evitare di utilizzare la stessa password per servizi differenti.

Per ovvie ragioni di sicurezza, occorre assolutamente evitare di rendere nota a terzi la propria password. Se ciò accadesse occorrerà cambiare immediatamente password. In particolare, se un Incaricato dovesse essere assente e accertata la necessità del servizio e l'impossibilità di dare ad altro Incaricato il servizio stesso, il Responsabile può autorizzare il Custode delle credenziali di aprire la busta contenente la password necessaria e affidarla ad altro Incaricato, registrando tale evento in modo opportuno. Al rientro dell'Incaricato temporaneamente assente, il Responsabile lo avvisa dell'evento e l'Incaricato provvederà a modificare immediatamente la password.

8.3.5 Criteri e procedure per garantire la sicurezza delle trasmissioni di dati

Al fine di garantire la sicurezza delle trasmissioni dei dati tra le sedi dislocate nel territorio, attraverso l'utilizzo di apparecchi di trasmissione dati, quali "Modem" e "Router", il Responsabile stabilisce, con il supporto tecnico dell'Amministratore del sistema, le misure tecniche da adottare in rapporto al rischio di intercettazione o di intrusione di "hacker" o "cracker" su ogni sistema collegato in rete pubblica. I criteri debbono essere stabiliti in relazione al tipo di rischio potenziale e in base al livello di tecnologia utilizzata e specificano le misure applicate contro l'intrusione e il contagio da virus.

8.3.6 Utilizzo di sistemi anti – intrusione

Di seguito vengono spiegati alcuni dei sistemi anti – intrusione utilizzati.

- **Firewall (lett. "Porta taglia fuoco")**
  È un software che controlla le connessioni, le porte, i dati in ingresso e in uscita, bloccando gli accessi e gli invii di dati non autorizzati.
- **Server proxy**
  Quando si naviga in Internet viene attribuito al nostro computer un indirizzo IP, che lo identifica in maniera univoca in tutto il mondo. Conoscendo il nostro IP, è possibile individuare la rete, la sottorete ed il provider a cui siamo connessi, ed in molti casi anche la nostra città. Per impedire di essere individuati con tanta precisione occorre utilizzare un server proxy. Un server proxy è un computer che si interpone fra il proprio computer e Internet, facendo da intermediario per tutto il traffico di dati sia in uscita che in entrata. In pratica i singoli computer non hanno accesso diretto alla rete esterna, ma solamente il proxy. Il che vuol dire che non saranno le identità dei singoli computer a viaggiare in rete, ma solamente quella del Proxy. Fino all'installazione di un server proxy è possibile utilizzare proxy esterni.
- **Verifica dei file con antivirus**
  Verificare sempre tutti i file che vengono introdotti nel nostro sistema con il software antivirus in dotazione. Se un file o un programma appena avviato sembra comportarsi in modo anomalo, occorre bloccarlo e rivolgersi all'Amministratore del sistema.
- **Controllo estensione file**
  Controllare sempre l'estensione dei file ricevuti.
- **Protezioni macro**
  Prima di avviare una macro collegata ad un file Word o Excel si può chiedere una conferma. Ciò lo si ottiene attivando la funzione "protezione macro" presente nel menu "Strumenti – Macro – Protezioni" e scegliendo il livello "Elevata".
  Inoltre, può essere buona pratica per non trasmettere virus macro e se non occorrono particolari funzionalità di Word, salvare i documenti in formato "Rich text format" (estensione ".rtf") o "Solo Testo" (estensione "txt").

8.4 MISURE DI SICUREZZA CONTRO IL RISCHIO DI TRATTAMENTO NON CONSENTITO

8.4.1 Personale autorizzato al trattamento dei dati e criteri di assegnazione dei permessi di accesso ai dati

Il Responsabile definisce i criteri per ogni incaricato per l'accesso e il trattamento dei dati e, in particolare:

- Inserimento di dati;
- Lettura e stampa di dati;
- Variazione di dati;
- Cancellazione di dati.

Il personale incaricato al trattamento dei dati viene nominato tramite comunicazione scritta, controfirmata per ricevuta, dal Titolare che ne conserva copia in luogo sicuro. Il Responsabile conserva un elenco degli incaricati che aggiorna ad ogni variazione. Per ogni incaricato che decade dal suo compito occorre attuare le procedure illustrate sopra sia per quanto riguarda gli accessi ai sistemi di trattamento dati automatici sia per quanto riguarda l'accesso ai luoghi fisici.

8.4.2 Verifiche periodiche delle condizioni per il mantenimento delle autorizzazioni

L'Amministratore del sistema, ogni anno entro il 15 settembre, verifica che tutte le condizioni di autorizzazioni, permessi e assegnazione degli Incaricati al trattamento dei dati siano congruenti con l'effettiva situazione esistente all'interno dell'Istituzione Scolastica. Ogni non conformità dovrà essere segnalata al Responsabile e al Titolare che provvederanno a ripristinare la corretta situazione.

8.5 MISURE DI SICUREZZA PER IL TRATTAMENTO DEI DATI EFFETTUATO CON STRUMENTI NON AUTOMATIZZATI

L'accesso agli archivi cartacei è consentito al solo personale autorizzato dal Responsabile e regolato mediante quanto descritto nei paragrafi precedenti (distribuzione delle chiavi di accesso ai locali e agli armadi).

Gli incaricati che trattano atti e documenti contenenti dati sensibili sono tenuti a conservarli e restituirli al termine delle operazioni.

In caso di allontanamento dal posto di lavoro, l'incaricato è tenuto a riporre in modo adeguato (contenitore chiuso) gli eventuali documenti oggetti di trattamento senza lasciarli incustoditi sulla scrivania o su qualsiasi altra postazione di lavoro.

Gli incaricati devono svolgere le operazioni di trattamento di dati nei locali previsti, in caso di trattamento in altri locali occorre trasportarli e custodirli in modo adeguato.

Le fotocopie o qualsiasi altro metodo di riproduzione cartacea dei documenti potranno essere effettuate solo dagli incaricati preposti (anche Collaboratori Scolastici a tale scopo nominati).

L'accesso ai luoghi fisici e in particolare agli archivi non è consentito dopo l'orario di chiusura, tranne casi di verificata urgenza e dietro autorizzazione del Responsabile.

8.6 MANUTENZIONE DELLE APPARECCHIATURE E DEI SISTEMI DI TRATTAMENTO DEI DATI

8.6.1 Manutenzione dei sistemi di elaborazione dei dati

L'Amministratore del sistema ha il compito di verificare ogni anno la situazione delle apparecchiature hardware installate con cui vengono trattati i dati, delle apparecchiature periferiche e, in particolare, dei dispositivi di collegamento con le reti pubbliche. Tale verifica ha lo scopo di controllare l'affidabilità del sistema per quanto riguarda:

1. la sicurezza dei dati trattati;
2. il rischio di distruzione o perdita;
3. il rischio di accesso non autorizzato o non consentito tenendo conto dell'evoluzione tecnica.

L'esito della verifica va messo per iscritto e consegnata al Responsabile del trattamento che la conserva in modo adeguato.

In caso di evidente rischio il Responsabile avvisa il Titolare affinché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme vigenti.

8.6.2 Manutenzione dei sistemi operativi

Prassi analoga a quella del paragrafo precedente va effettuata per i sistemi operativi installati sulle apparecchiature con le quali vengono trattati i dati. In questo caso occorre tenere conto di:

1. disponibilità di nuove versioni migliorative dei sistemi operativi utilizzati;
2. segnalazioni di patch, fix o system – pack per la rimozione di errori o malfunzionamenti;
3. segnalazioni di patch, fix o System – pack per l'introduzione di maggiori sicurezze contro i rischi d'intrusione o di danneggiamento dei dati.

L'esito della verifica va messo per iscritto e consegnata al Responsabile del trattamento che la conserva in modo adeguato.

In caso di evidente rischio il Responsabile avvisa il Titolare affinché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme vigenti.

8.6.3 Manutenzione delle applicazioni software

Sono soggette alle verifiche di cui al paragrafo precedente anche le applicazioni software installate sulle apparecchiature con cui vengono trattati i dati. Anche in questo caso occorre tenere conto delle nuove versioni migliorative che consentono maggiore sicurezza contro i rischi d'intrusione o di danneggiamento dei dati.

L'esito della verifica va messo per iscritto e consegnata al Responsabile del trattamento che la conserva in modo adeguato.

In caso di evidente rischio il Responsabile avvisa il Titolare affinché siano presi gli opportuni provvedimenti allo scopo di assicurare il corretto trattamento dei dati in conformità alle norme vigenti.

9 PIANO DI FORMAZIONE DEL PERSONALE AUTORIZZATO AL TRATTAMENTO DEI DATI

Al Responsabile del trattamento è affidato il compito di verificare ogni anno, entro il 31 agosto, le necessità di formazione del personale Incaricato al trattamento dei dati, con lo scopo di fornire ogni informazione necessaria a migliorare la sicurezza di trattamento dei dati, e del personale incaricato di effettuare periodicamente le operazioni di back – up delle banche dei dati trattati.

Per ogni incaricato del trattamento, il Responsabile definisce, sulla base dell'esperienza e delle sue conoscenze, ed in funzione anche di eventuali opportunità offerte dall'evoluzione tecnologica, se è necessaria una formazione tecnica adeguata e redige un "Piano di formazione per la sicurezza" che deve essere trasmesso in copia controllata al Titolare.

In ogni caso la formazione degli incaricati dovrà prevedere sicuramente i seguenti punti:

1. una analisi dettagliata ed aggiornata delle vigenti disposizioni di legge, con riferimenti anche alle normative europee;
2. disposizioni legislative in tema di tutela dei dati e criminalità informatica;
3. analisi dettagliata del D. Lgs 196/03;
4. analisi e spiegazione dei ruoli: Titolare, Responsabile, Incaricato, Amministratore di sistema, Custode delle credenziali, Interessato;
5. panoramica sugli adempimenti ex legge 675/96: notificazione, rapporti con gli interessati, rapporti con il Garante;
6. l'ufficio del Garante;
7. misure minime ed appropriate di sicurezza con particolare riferimento a criteri logici, fisici ed organizzativi per la protezione dei sistemi informativi, prevenzione e contenimento del danno, strumenti di protezione hardware e software, contenitori di sicurezza, sistemi anti – intrusione, importanza e modalità di realizzazione delle operazioni di back – up, ecc.

10 GESTIONE DEGLI STATI DI CRISI E RISPOSTA

Per gestione della crisi s'intende il coordinamento complessivo della risposta organizzativa ad una possibile crisi in modo efficace e tempestivo, con lo scopo di evitare o minimizzare i danni alla reputazione ed alla capacità di operare dell'Istituzione Scolastica.

In caso di incidente devono essere considerate le seguenti priorità:

1. evitare danni diretti alle persone;
2. proteggere l'informazione sensibile o proprietaria;
3. evitare danni economici;
4. limitare i danni all'immagine dell'Istituzione Scolastica.

Garantita l'incolumità fisica delle persone, le situazioni di crisi devono immediatamente essere comunicate all'Amministratore del sistema e al Responsabile che provvederanno a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema (nel caso di sistemi windows staccare la presa dalla corrente);
4. ripristinare il sistema;
5. effettuare test di operatività;
6. ripristinare e far riprendere l'operatività normale;
7. documentare tutte le operazioni compilando un report da consegnare al Titolare.

Per consentire valide strategie di ripristino occorre prevedere:

1. un regolare back – up ed un sistema di archiviazione delle informazioni in un ambiente protetto, insieme alle licenze software, le system configuration e le altre informazioni necessarie;
2. una ridondanza di data storage (immagazzinamento dei dati), communication path (linee di comunicazione), alimentazioni e componenti di sistema che riducano la probabilità di blocco dei sistemi;
3. il possesso di macchine equivalenti ai server per un loro possibile utilizzo in tale veste;
4. l'acquisizione di un armadio ignifugo per conservare le copie di back – up delle banche dati.

Il piano proposto garantisce che il ripristino dei dati avviene al massimo in una settimana dal verificarsi dell'evento.

11 PIANO DI VERIFICA DELLE MISURE ADOTTATE

La bontà delle misure adottate deve essere periodicamente verificata. In particolare:

1. verificare l'accesso fisico ai locali ove si svolge il trattamento (a cura del Responsabile, ogni 2 mesi);
2. verificare il corretto utilizzo delle password e dei profili di accesso degli incaricati, prevedere la disattivazione dei codici di accesso non utilizzati per più di sei mesi (a cura dell'Amministratore del sistema, ogni 6 mesi);
3. verificare l'integrità dei dati e delle loro copie di back – up (a cura del Responsabile, ogni mese);
4. verificare che i sistemi informatici siano regolarmente aggiornati in termini di patch ed antivirus (a cura dell'Amministratore del sistema, ogni 2 mesi);
5. verificare la bontà di conservazione dei documenti cartacei (a cura del Responsabile, ogni 6 mesi);
6. verificare la distruzione dei supporti magnetici che non possono essere più riutilizzati (a cura del Responsabile, ogni mese);

7. verificare il livello di formazione degli Incaricati, prevedere sessioni di aggiornamento anche in relazione all'evoluzione tecnica e tecnologica avvenuta nell'Istituzione Scolastica (a cura del Responsabile, ogni anno).

Di queste verifiche viene redatto processo verbale da conservare in modo adeguato dal Responsabile.

12 REVISIONI

Tabella delle Revisioni

N° Protocollo	Tipo di modifica	Data emissione revisione
2507/A28	Il documento è stato completamente rifatto	31 – 03 – 2009
1999/A28	Il documento è stato rivisto	13 – 03 – 2010
1375/A28	I documento è stato rivisto	19 – 02 – 2011

ISTITUTO TECNICO COMMERCIALE E PER GEOMETRI
" V. PARETO"
Via Annecchino, 252 – 80078 Pozzuoli (NA)
Tel.: 081/8664962; **Fax**: 081/5046777
C. M.: NATD130003; **e–mail**: natd130003@istruzione.it

INDICE