Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)
ALLEGATO 3 – Misure, incident response, ripristino

Istituto Comprensivo "Andrea Testore"

Tabella 1 - Connettività internet

Connettività	Apparecchiature di comunicazione	Provider
ADSL	Router Pirelli Alice	Telecom Italia Alice

Tabella 2 - Descrizione Personal Computer[1]

Identificativo del PC	Tipo PC	Sistema operativo	Software utilizzato	rete
01	Pentium4 3 Ghz, Olidata, 512 Mb ram, 160 Gb Hd.	Win Xp Pro Sp2	Sissi, Office 2003 Basic Microsoft, Inps 2000, Entratel, Argo , Protocollo informatico	Si
02	Pentium4 3 Ghz, Olidata, 512 Mb ram, 160 Gb Hd.	Win Xp Pro Sp2	Sissi, Office 2003 Basic Microsoft, Argo, Protocollo informatico	Si
03	Pentium4 3 Ghz, Olidata, 512 Mb ram, 160 Gb Hd.	Win Xp Pro Sp2	Sissi, Office 2003 Basic Microsoft, Argo, Protocollo informatico	Si
04	Pentium4 3 Ghz, Olidata, 512 Mb ram, 160 Gb Hd.	Win Xp Pro Sp2	Sissi, Office 2003 Basic Microsoft, Argo Protocollo informatico	Si
05	Pentium4 3 Ghz, Olidata, 512 Mb ram, 160 Gb Hd.	Win Xp Pro Sp2	Office 2003 Basic Microsoft	Si
06	Pentium4 3 Ghz,	Win Xp Pro Sp2	Sissi, Office 2003 Basic	Si

[1] I PC descritti in questa tabella **non** prendono in considerazione quelli presenti nei laboratori didattici
Note: Gli applicativi del programma Argo sono : Alunni sui PC 1-2-3-4-6-7
Personale sui PC 1-2-3-4-6-7
Stipendi sui PC 1-2-3-7
Fisco sui PC 1-7

	Olidata, 512 Mb ram, 160 Gb Hd.		**Microsoft, Argo, Protocollo informatico**	
07	**Pentium 4 i server di rete, 2 dischi sata raid 1 mirroring**	**Win 2003 server R2**	**Sissi in rete, Argo con database Sybase**	**Si**

MISURE DI CARATTERE ELETTRONICO/INFORMATICO

Le misure di carattere elettronico/informatico[2] adottate sono:

- Il server utilizza due dischi configurati in mirroring hardware per permettere maggiore sicurezza dei dati e tempi più rapidi di ripristino in caso di malfunzionamenti dovuti ai dischi.
- Il computer adibito precedentemente a server si trova dismesso in locale ad accesso controllato (deposito attrezzature in disuso).La sua scheda madre è stata riutilizzata sul pc docenti dell'aula di informatica. Nel momento in cui venisse individuato un possibile reimpiego, si procederà alla sostituzione del disco fisso e alla reinstallazione dei software licenziati. Il disco sostituito verrà custodito in cassaforte quale backup storico. In caso di rottamazione si procederà alla rottura meccanica dello stesso per renderlo definitivamente illeggibile.Tale procedura sarà adottata per tutti i computer dismessi utilizzati per scopi amm.vi e didattici e in occasione della eventuale eliminazione dall'inventario dei beni mobili della scuola si redigerà un sintetico verbale in cui si annoteranno le modalità di cancellazione dei dati dall'hard disk o le modalità di distruzione del supporto stesso.
- presenza di gruppi di continuità elettrica per il server: è presente un gruppo di continuità sul server e uno sugli apparati di rete.
- Le *copie di sicurezza sono automatiche giornaliere e storiche mensili e trimestrali; richiedono solo il controllo dell'avvenuta funzionalità.* Alla data di questo documento i responsabili delle copie sono indicati nell'Allegato 1 relativo al censimento dei trattamenti dei dati.I backup sono centralizzati sul server 07 e su due dischi esterni scollegabili in modo da poter conservare uno dei due dischi in luogo protetto (cassaforte esistente nell'Ufficio del Dsga).Periodicamente i dischi esterni vengono sostituiti e conservati in cassaforte onde far fronte a rischi di perdita totale delle apparecchiature.Inoltre ogni 7 giorni sul server viene effettuato il backup del programma ministeriale Sissi in Rete (in corso di dismissione),utilizzando l'apposita procedura di utilità.
- E' utilizzato un firewall di produzione Symantec con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet;
- definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows XP, di seguito specificate: è presente una politica di gestione delle password che prevede la sostituzione ogni 6 mesi, le password sono formate da almeno otto caratteri alfanumerici non riferibili all'utente, le password non vengono comunicate ad altri utenti non autorizzati, sono

[2] Le misure di carattere elettronico/informatico sono quelle in grado di segnalare gli accessi agli elaboratori, agli applicativi, ai dati e alla rete, di gestire le copie di salvataggio dei dati e degli applicativi, di assicurare l'integrità dei dati, di proteggere gli elaboratori da programmi volutamente o involontariamente ritenuti dannosi.

presenti password sul bios che impediscono l'accensione delle macchine e password di sistema che impediscono l'accesso ai dati e ai programmi, sono presenti password di applicativo che impediscono e gestiscono le priorità di accesso ai programmi;

- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows 9x e Windows Me e comunque, sui computer non elencati nella precedente tabella;
- installazione di un sistema antivirus su tutti le postazioni di lavoro, configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico e la scansione periodica dei supporti di memoria: è presente un antivirus (Microsoft Security Essentials) che controlla i file in tempo reale di accesso e si aggiorna automaticamente;
- definizione delle regole per la gestione di strumenti elettronico/informatico, di seguito riportate;
- definizione delle regole di comportamento per minimizzare i rischi da virus, di seguito riportate;
- separazione della rete locale delle segreterie da quella dei laboratori didattici: la rete locale della segreteria è fisicamente separata da quella dei laboratori.

REGOLE PER LA GESTIONE DELLE PASSWORD[3]

Tutti gli incaricati del trattamento dei dati personali accedono al sistema informativo per mezzo di un codice identificativo personale (in seguito indicato user-id) e password personale.
User-id e password iniziali sono assegnati, dal custode delle password.
User-id e password sono strettamente personali e non possono essere riassegnate ad altri utenti.
L'user-id è costituita da 8 caratteri che corrispondono alle prime otto lettere del cognome ed eventualmente del nome. In caso di omonimia si procede con le successive lettere del nome.
La password è composta da 8 caratteri alfanumerici. Detta password non contiene, né conterrà, elementi facilmente ricollegabili all'organizzazione o alla persona del suo utilizzatore e deve essere autonomamente modificata dall'incaricato al primo accesso al sistema e dallo stesso consegnata in una busta chiusa al custode delle password, il quale provvede a metterla nella cassaforte in un plico sigillato.
Ogni sei mesi (tre nel caso di trattamento dati sensibili) ciascun incaricato provvede a sostituire la propria password e a consegnare al custode delle password una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il custode delle password provvederà a sostituire la precedente busta con quest'ultima.
Le password verranno automaticamente disattivate dopo tre mesi di non utilizzo.
Le password di amministratore di tutti i PC che lo prevedono sono assegnate dall'amministratore di sistema, esse sono conservate in busta chiusa nella cassaforte. In caso di necessità l'amministratore di sistema è autorizzato a intervenire sui personal computer.
In caso di manutenzione straordinaria possono essere comunicate, qualora necessario, dall'amministratore di sistema al tecnico/sistemista addetto alla manutenzione le credenziali di autenticazione di servizio. Al termine delle operazioni di manutenzione l'amministratore di sistema deve ripristinare nuove credenziali di autenticazione che

[3] La password è un elemento fondamentale per la sicurezza delle informazioni. La robustezza delle password è il meccanismo più importante per proteggere i dati; un corretto utilizzo della password è a garanzia dell'utente.

devono essere custodite in cassaforte.
Le disposizioni di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati personali e/o sensibili:

- le password assegnate inizialmente e quelle di default dei sistemi operativi, prodotti software, ecc. devono essere immediatamente cambiate dopo l'installazione e al primo utilizzo;
- per la definizione/gestione della password devono essere rispettate le seguenti regole:
  - la password deve essere costituita da una sequenza di minimo otto caratteri alfanumerici e non deve essere facilmente individuabile;
  - deve contenere almeno un carattere alfabetico ed uno numerico;
  - non deve contenere più di due caratteri identici consecutivi;
  - non deve contenere lo user-id come parte della password;
  - al primo accesso la password ottenuta dal custode delle password deve essere cambiata; la nuova password non deve essere simile alla password precedente;
  - la password deve essere cambiata almeno ogni sei mesi, tre nel caso le credenziali consentano l'accesso ai dati sensibili o giudiziari;
  - la password termina dopo sei mesi di inattività;
  - la password è segreta e non deve essere comunicata ad altri;
  - la password va custodita con diligenza e riservatezza;
  - l'utente deve sostituire la password, nel caso ne accertasse la perdita o ne verificasse una rivelazione surrettizia.

REGOLE PER LA GESTIONE DI STRUMENTI ELETTRONICO/INFORMATICO
Per gli elaboratori che ospitano archivi (o hanno accesso tramite la rete) con dati personali sono adottate le seguenti misure:

- l'accesso agli incaricati ed agli addetti alla manutenzione è possibile solo in seguito ad autorizzazione scritta;
- gli hard disk non sono condivisi in rete se non temporaneamente per operazioni di copia;
- tutte le operazioni di manutenzione che sono effettuate on-site avvengono con la supervisione dell'incaricato del trattamento o di un suo delegato;
- le copie di backup realizzate su disco esterno usb2 sono conservate in armadio metallico con chiusura a chiave nell'ufficio del Direttore
- divieto di utilizzare floppy disk come mezzo per il backup;
- divieto per gli utilizzatori di strumenti elettronici di lasciare incustodito, o accessibile, lo strumento elettronico stesso. A tale riguardo, per evitare errori e dimenticanze, è adottato uno screensaver automatico dopo 10 minuti di non utilizzo, con ulteriore password segreta per la prosecuzione del lavoro.
- divieto di memorizzazione di archivi con dati sensibili di carattere personale dell'utente sulla propria postazione di lavoro non inerenti alla funzione svolta;
- divieto di installazione di software di qualsiasi tipo sui personal computer che contengono archivi con dati sensibili senza apposita autorizzazione scritta da parte del responsabile del trattamento dati;
- divieto di installazione sui personal computer di accessi remoti di qualsiasi tipo mediante modem, linee telefoniche o altri mezzi idonei.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.
La stampa di documenti contenenti dati sensibili è effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

Il fax si trova in locale ad accesso controllato (Ufficio di Segreteria) e l'utilizzo è consentito unicamente agli incaricati del trattamento *(vedi allegato 1).*

La manutenzione degli elaboratori, che può eventualmente prevedere il trasferimento fisico presso un laboratorio riparazioni, è autorizzata solo a condizione che il fornitore del servizio dichiari per iscritto di avere redatto il documento programmatico sulla sicurezza e di aver adottato le misure minime di sicurezza previste dal disciplinare.

REGOLE DI COMPORTAMENTO PER MINIMIZZARE I RISCHI DA VIRUS[4]

Per minimizzare il rischio da virus informatici, gli utilizzatori dei PC adottano le seguenti regole:

- limitare lo scambio fra computer di supporti rimovibili (floppy, cd, zip) contenenti file con estensione EXE, COM, OVR, OVL, SYS, DOC , XLS;
- controllare (scansionare con un antivirus aggiornato) qualsiasi supporto di provenienza sospetta prima di operare su uno qualsiasi dei file in esso contenuti;
- evitare l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza, ovvero divieto di "scaricare" dalla rete internet ogni sorta di file, eseguibile e non. La decisione di "scaricare" può essere presa solo dal responsabile del trattamento;
- disattivare gli Activex e il download dei file per gli utenti del browser Internet Explorer;
- disattivare la creazione di nuove finestre ed il loro ridimensionamento e impostare il livello di protezione su "chiedi conferma" (il browser avvisa quando uno script cerca di eseguire qualche azione);
- attivare la protezione massima per gli utenti del programma di posta Outlook Express al fine di proteggersi dal codice html di certi messaggi e-mail (buona norma è visualizzare e trasmettere messaggi in formato testo poiché alcune pagine web, per il solo fatto di essere visualizzate possono infettare il computer);
- non aprire gli allegati di posta se non si è certi della loro provenienza, e in ogni caso analizzarli con un software antivirus. Usare prudenza anche se un messaggio proviene da un indirizzo conosciuto (alcuni virus prendono gli indirizzi dalle mailing list e della rubrica di un computer infettato per inviare nuovi messaggi "infetti");
- non cliccare mai un link presente in un messaggio di posta elettronica da provenienza sconosciuta,(in quanto potrebbe essere falso e portare a un sito-truffa);
- non utilizzare le chat;
- consultare con periodicità settimanale la sezione sicurezza del fornitore del sistema operativo e applicare le patch di sicurezza consigliate;
- non attivare le condivisioni dell'HD in scrittura.
- seguire scrupolosamente le istruzioni fornite dal sistema antivirus nel caso in cui tale sistema antivirus abbia scoperto tempestivamente il virus (in alcuni casi esso è in grado di risolvere il problema, in altri chiederà di eliminare o cancellare il file infetto);
- avvisare l'Amministratore di sistema nel caso in cui il virus sia stato scoperto solo dopo aver subito svariati malfunzionamenti della rete o di qualche PC, ovvero in ritardo (in questo caso è possibile che l'infezione abbia raggiunto parti vitali del sistema);

[4] Le più recenti statistiche internazionali citano il virus informatico come la minaccia più ricorrente ed efficace

- conservare i dischi di ripristino del proprio PC (creati con l'installazione del sistema operativo, o forniti direttamente dal costruttore del PC);
- conservare le copie originali di tutti i programmi applicativi utilizzati e la copia di backup consentita per legge;
- conservare la copia originale del sistema operativo e la copia di backup consentita per legge;
- conservare i driver delle periferiche (stampanti, schede di rete, monitor ecc. fornite dal costruttore).

Nel caso di sistemi danneggiati seriamente da virus l'Amministratore procede a reinstallare il sistema operativo, i programmi applicativi ed i dati; seguendo la procedura indicata:

1. formattare l'Hard Disk,definire le partizioni e reinstallate il Sistema Operativo. (molti produttori di personal computer forniscono uno o più cd di ripristino che facilitano l'operazione);
2. installare il software antivirus, verificate e installare immediatamente gli eventuali ultimi aggiornamenti;
3. reinstallare i programmi applicativi a partire dai supporti originali;
4. effettuare il RESTORE dei soli dati a partire da una copia di backup recente. NESSUN PROGRAMMA ESEGUIBILE DEVE ESSERE RIPRISTINATO DALLA COPIA DI BACKUP: potrebbe essere infetto;
5. effettuare una scansione per rilevare la presenza di virus nelle copie dei dati;
6. ricordare all'utente di prestate particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.

INCIDENT RESPONSE E RIPRISTINO[5]

Tutti gli incaricati del trattamento dei dati devono avvisare tempestivamente il responsabile della sicurezza informatica o l'amministratore di sistema o il responsabile del trattamento dei dati, nel caso in cui constatino le seguenti anomalie:

- discrepanze nell'uso degli user-id;
- modifica e sparizione di dati;
- cattive prestazioni del sistema (così come percepite dagli utenti);
- irregolarità nell'andamento del traffico;
- irregolarità nei tempi di utilizzo del sistema;
- quote particolarmente elevate di tentativi di connessione falliti.

In caso di incidente sono 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'organizzazione.

Garantita l'incolumità fisica alle persone si procedere a:

1. isolare l'area contenente il sistema oggetto dell'incidente;
2. isolare il sistema compromesso dalla rete;
3. spegnere correttamente il sistema oggetto dell'incidente(vedi tabella 3). **Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso[6];**

[5] Un incidente può essere definito come un evento che produce effetti negativi sulle operazioni del sistema e che si configura come frode, danno, abuso, compromissione dell'informazione, perdita di beni.

[6] E' indispensabile che per una eventuale indagine venga assicurata l'integrità e la sicurezza dello stato del sistema in oggetto e quindi non venga introdotta alcuna alterazione ai dati residenti nel sistema medesimo; un ripristino

4. documentare tutte le operazioni.

Se l'incidente è dovuto ad imperizia del personale o ad eventi accidentali, ovvero quando non vi è frode, danno, abuso e non è configurabile nessun tipo di reato, il ripristino può essere effettuato, a cura dell'amministratore di sistema, direttamente sugli hard disk originali a partire dalle ultime copie di backup ritenute valide.
Altrimenti il titolare del trattamento, il responsabile del trattamento e l'amministratore di sistema coinvolgeranno esperti e/o autorità competenti. La successiva fase di indagine e di ripristino del sistema sarà condotta da personale esperto di incident response, tenendo presente quanto sotto indicato:

1. eseguire una copia bit to bit degli hard disk del sistema compromesso;
2. se l'incidente riguarda i dati il restore dei dati può avvenire sulla copia di cui al punto 1 precedente a partire dalle ultime copie di backup ritenute valide;
3. se l'incidente riguarda il sistema operativo o esiste la possibilità che sia stato installato software di tipo MMC (vedere Allegato 2) il ripristino deve essere effettuato reinstallando il sistema operativo su nuovo supporto.

Tabella 3 - Procedure di spegnimento

Sistema operativo	Azione
Windows 98/NT/2000/XP	1. Fotografare lo schermo e documentare i programmi che sono attivi. 2. Staccare la spina dalla presa di corrente.

Nota: *(fonte U.S. Departement of Energy)*

affrettato del sistema potrebbe alterare le prove dell'incidente.