

PIANO OPERATIVO PER L'ADOZIONE DELLE MISURE MINIME DI SICUREZZA NEL TRATTAMENTO DEI DATI PERSONALI NELL'AMBITO DELLE ATTIVITA' DELLA SCUOLA..... AI SENSI DEL DPR 318/99 PER L'ANNO 2003

Indice

1 Premessa

- 1.1 Definizioni
- 1.2 Normativa di riferimento
- 1.3 Sedi
- 1.4 Titolare del trattamento
- 1.5 Responsabili
- 1.6 Incaricati
- 1.7 Il sistema informativo

2 Analisi del rischio

- 2.1 Il data base
- 2.2.1 Archivi cartacei
- 2.2.2 Archivi informatici
- 2.2.3 Misure di sicurezza relative agli accessi
- 2.3 Rischio logico

3 Misure minime di sicurezza adottate

- 3.1 Archivi su supporto cartaceo
 - 3.1.1 Norme generali
 - 3.1.2 Norme per i dati sensibili e giudiziari
- 3.2 Archivi su supporto informatico per elaboratore collegati in rete locale
 - 3.2.1 Sicurezza fisica dei computert
 - 3.2.2 Difesa da accessi non autorizzati da rete geografica
 - 3.2.3 Codice indentificativo degli utenti del sitema informativo
 - 3.2.4 Protezione degli archivi informatici contenenti dati sensibili e giudiziari
 - 3.2.5 Salvataggio dei dati di backup
 - 3.2.6 La cassaforte
 - 3.2.7 Protezione da virus informatici
 - 3.2.8 Protezione da rischi durante la trasmisioine dati
 - 3.2.9 Uso di programmi di sniffer e port scanning
 - 3.2.10 Riutilizzazione dei supporti di memorizzazione dei dati sensibili

4 Formazione

5 Incident response informatico

6 Piano di attività annuale in materia di sicurezza

7 Aggiornamento del piano

8 Allegati

1 Premessa

Scopo di questo documento è stabilire **le misure di sicurezza organizzative, fisiche e logiche da adottare** affinché siano rispettati gli obblighi, in materia di sicurezza, previsti dalla legge 675/96 sulla protezione dei dati personali (Legge sulla Privacy) e dal DPR 318/99.

Il piano prevede un'azione di formazione continua per tutti i dipendenti finalizzata a promuovere la cultura della sicurezza, indispensabile a garantire l'integrità e la riservatezza delle informazioni, siano esse conservate su supporti cartacei o informatici.

In particolare tale piano persegue l'obiettivo di:

- minimizzare la probabilità di appropriazione, danneggiamento o distruzione anche non voluta di apparecchiature informatiche o archivi informatici o cartacei contenenti dati sensibili;
- minimizzare la probabilità di accesso, comunicazione o modifiche non autorizzate alle informazioni sensibili;
- minimizzare la probabilità che i trattamenti dei dati sensibili siano modificati senza autorizzazione.

Il presente Documento Programmatico sulla Sicurezza delle Informazioni deve essere divulgato e spiegato a tutti gli incaricati.

Eventuali situazioni di deviazione accertate rispetto a quanto precisato nel presente documento dovranno essere rimosse nel più breve tempo possibile.

1.1 Definizioni

DATO PERSONALE: qualunque informazione riferibile, anche indirettamente, a persona fisica, persona giuridica, ente o associazione.

DATO ANONIMO: il dato che in origine, o a seguito di trattamento, non può essere associato a un interessato identificato o identificabile.

DATI SENSIBILI: i dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati personali.

INTERESSATO: il soggetto al quale si riferiscono i dati personali.

RESPONSABILE DEL TRATTAMENTO: il soggetto preposto dal titolare al trattamento dei dati personali. La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto che fornisce, per esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza

RESPONSABILE DEL SISTEMA INFORMATIVO: il soggetto preposto dal titolare alla gestione della rete (amministratore di rete). La designazione di un responsabile è facoltativa e non esonera da responsabilità il titolare, il quale ha comunque l'obbligo di

impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il responsabile deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali, deve inoltre conoscere le vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

TITOLARE: il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

1.2 Normativa di riferimento

- Legge 675/1996;
- D.P.R. 318/1999
- Legge 325/2000;
- Regolamento scolastico, policy di utilizzo della rete.

1.3 Sedi

Il presente Documento Programmatico sulla Sicurezza delle Informazioni si applica alla sede centrale

.....

e alla sede coordinata

.....

1.4 Titolare del trattamento

Il titolare del trattamento è l'istituto scolastico e la titolarità è esercitata dal dirigente scolastico, tra i compiti che la legge gli assegna e che non sono delegabili, è prevista la vigilanza sul rispetto da parte dei Responsabili delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

1.5 Responsabili

Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le seguenti responsabilità:

- promuovere lo sviluppo, la realizzazione ed il mantenimento dei programmi di sicurezza contenuti nel presente Documento Programmatico sulla Sicurezza dei Dati Personali;
- informare il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti;
- promuovere lo svolgimento di un continuo programma di addestramento degli Incaricati del Trattamento e mantenere attivo un programma di controllo e monitoraggio della corrispondenza con le regole di sicurezza.
- Collaborare con il responsabile del sistema informativo.

Il responsabile del sistema informativo ha le seguenti responsabilità:

- sovrintendere al funzionamento della rete, comprese le

- apparecchiature di protezione (firewall, filtri);
- collaborare con il responsabile del trattamento dei dati personali;
- monitorare lo stato dei sistemi, con particolare attenzione alla sicurezza;
- informare il Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali incidenti;

1.6 Incaricati

Gli Incaricati del trattamento dei dati personali, con specifico riferimento alla sicurezza, hanno le seguenti responsabilità:

- svolgere le attività previste dai trattamenti secondo le prescrizioni contenute nel presente Documento Programmatico sulla Sicurezza e le direttive del responsabile del trattamento dei dati;
- non modificare i trattamenti esistenti o introdurre nuovi trattamenti senza l'esplicita autorizzazione del responsabile del trattamento dei dati;
- rispettare e far rispettare le norme di sicurezza per la protezione dei dati personali;
- informare il responsabile in caso di incidente di sicurezza che coinvolga dati sensibili e non.

1.7 Il sistema informativo (descrizione della/e rete/i dell'istituto/i - sezione da personalizzare)

Il Sistema Informativo della Scuola..... è costituito da due reti locali separate, quella didattica e quella amministrativa, rispettivamente composte da 50 e 14 posti di lavoro costituiti da personal computer Intel Pentium di varie potenze e capacità elaborative con sistemi operativi Windows 95/98, Windows XP, Linux.

Rete amministrativa

Tutti i posti di lavoro sono connessi in rete locale mediante switch di dominio e cablaggio Ethernet UTP RJ45 con protocollo TCP/IP. Otto personal computer sono riservati al personale dirigente e di segreteria. Quattro personal computer, localizzati in sala insegnanti, sono riservati ai docenti. I due server vengono utilizzati uno (Windows 200) per i dati relativi all'applicativo SSSI in rete, l'altro (Linux) per i docenti, relazioni, giudizi ecc. I server si trovano, con le apparecchiature di continuità (gruppo di), di comunicazione (router) e di protezione (firewall), in apposito locale adiacente ai locali della segreteria.

Tutti i computer sono dotati di indirizzo IP statico in classe C, assegnato dal responsabile del sistema informativo.

La connettività internet avviene attraverso RUPAR con indirizzo IP statico in classe A

La separazione/protezione tra la rete RUPAR e quella amministrativa è realizzata attraverso un firewall (vedi in seguito caratteristiche).

Rete didattica

Tutti i posti di lavoro sono connessi in rete locale mediante switch di dominio, hub e cablaggio Ethernet UTP RJ45 con protocollo TCP/IP, i computer sono localizzati in quattro locali.

Tutti i computer sono dotati di indirizzo IP statico in classe C, assegnati dai responsabili dei laboratori.

La connettività internet avviene attraverso la RUPAR con indirizzo IP statico in classe A.

La separazione/protezione tra le rete RUPAR e quella didattica è realizzata per mezzo di un firewall (vedi in seguito caratteristiche).

Policy

Tutti gli utenti della rete devono rispettare le norme previste nel documento policy di utilizzo della rete.

La sede coordinata di.....è fornita di due reti locali separate, una amministrativa composta di tre personal computer e una didattica composta di dodici personal computer.

La connettività internet, per entrambe le reti, è fornita dal provider.....

Il server (win2000) si trova nel locale segreteria ed è provvisto di gruppo di continuità.

Tutti i personal computer sono dotati di indirizzo IP statico in classe C (assegnato dal responsabile del sistema informativo), la separazione/protezione dalla rete internet è effettuata per mezzo di firewall (vedi sotto).

Il backup degli archivi in uso avviene in sede locale con conservazione dei supporti in apposito armadio con chiave situato nell'unico locale adibito a segreteria.

VPN

E' prevista, nel prossimo anno solare, la sperimentazione di una rete privata virtuale (VPN) tra le segreterie delle due sedi, a tal scopo i firewall sono già stati configurati per permettere tale collegamento.

2 Analisi del rischio

I rischi a cui sono sottoposti gli archivi presenti nella scuola si possono suddividere in rischi fisici e logici. Alla prima tipologia appartengono tutti gli archivi a supporto cartaceo e in parte quelli su supporto informatico. Alla seconda tipologia appartengono quelli che utilizzano elaboratori elettronici ed in specie quelli connessi in rete, sia locale che geografica.

2.1 Il Data Base

Per poter analizzare i rischi connessi all'utilizzo di archivi contenenti sia dati comuni che dati sensibili è stato realizzato un data base il cui scopo è quello di censire i trattamenti dei dati, sensibili e non. Al Data Base possono accedere il dirigente scolastico e/o suo delegato, il direttore dei servizi generali e amministrativi e i responsabili del trattamento dei dati e del sistema informativo per mezzo di password personale per l'inserimento e l'aggiornamento dei dati.

Tracciato record:

Nome campo	Tipo	Descrizione
Ufficio	TAB	Identifica l'ufficio in cui si trova l'archivio
Identificativo	TEXT	Nome dell'archivio (p.es. Anagrafe alunni)
Descrizione	MEMO	Breve descrizione dell'archivio
Soggetti	TEXT	Soggetti ai quali si riferiscono i dati
Tipologia	TAB	Personale, Sensibile, Anonimo
Supporto	TAB	Cartaceo, Informatico
Uso	TEXT	Per cosa vengono utilizzati i dati
Operatori	MEMO	Nome degli incaricati del trattamento
Conservazione	TEXT	Luogo di conservazione dei dati cartacei (armadio, raccoglitore ecc.)
Supporto	TAB	Supporto informatico (FD, HD,CD, ZIP, Memoria flash)
PC	TAB	Stand alone, in rete, server
Backup	TAB	Supporto del backup
Frequenza	TAB	Frequenza del backup
Responsabile	TEXT	Responsabile dell'archivio
Compilatore	TEXT	Compilatore
Data	DATA	Data compilazione

Il Data Base dovrà essere costantemente tenuto aggiornato a cura del delegato del dirigente scolastico e/o dal responsabile del trattamento; i dati in esso contenuti saranno utilizzati per l'analisi dei rischi e delle misure minime da adottare per scongiurare l'utilizzo non legittimo degli archivi e la perdita di informazioni.

2.2 *Rischio fisico*

Il furto o il danneggiamento delle apparecchiature informatiche, la diffusione o distruzione non autorizzata di informazioni personali e l'interruzione dei processi informatici possono esporre l'istituto al rischio di violare la legge 675/96.

2.2.1 *Archivi cartacei*

Gli archivi cartacei di norma sono conservati in armadi con chiave, i rischi fisici a cui

sono sottoposti sono i seguenti:

- Accesso agli uffici e agli archivi di persone esterne all'ente;
- Smarrimento per incuria da parte del personale;
- Furto;
- Visura e/o copiatura da parte di personale non autorizzato;
- Perdita parziale o totale a causa di incendi o allagamenti;
- Perdita parziale o totale per il degrado naturale del supporto (invecchiamento);
- Atti di vandalismo.

2.2.2 Archivi informatizzati

Gli archivi informatizzati risiedono su elaboratori elettronici, i rischi fisici a cui sono soggetti sono i seguenti:

- Distruzione fisica dell'elaboratore per eventi esterni allo stesso quali incendi, allagamenti, sbalzi di corrente;
- Distruzione fisica dei supporti fisici di backup dei dati per eventi esterni quali incendi, allagamenti, sbalzi di corrente;
- Guasti hardware dell'elaboratore tali da impedire il recupero degli archivi che si trovano sugli hard disk;
- Furto dell'elaboratore e/o dei supporti di backup dei dati;
- Perdita di dati dovuta a imperizia del personale addetto;
- Accesso agli elaboratori da parte di personale non autorizzato;
- Interruzione dei servizi di connessione fisica alla rete (linee telefoniche, router, modem, switch, hub);
- Atti di vandalismo.

2.2.3 Misure di sicurezza relative agli accessi fisici

Sono definite aree ad accesso controllato quei locali che contengono apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati sensibili e apparecchiature di telecomunicazione) e archivi informatici e/o cartacei contenenti dati sensibili; tali aree:

- devono essere all'interno di aree sotto la responsabilità della istituto.....;
- deve essere chiaramente identificato un "responsabile dell'area";
- Il locale deve essere chiuso anche se presidiato, le chiavi sono custodite a cura del "responsabile dell'area".

Inoltre:

- l'accesso deve essere consentito solo alle persone autorizzate;
- l'accesso deve essere possibile solo dall'interno dell'area sotto la responsabilità dell'istituto scolastico.....;
- i locali devono essere provvisti di sistema di allarme.

In generale per i locali che contengono documenti riguardanti dati sensibili, cartacei e/o informatici devono essere definite le seguenti regole di gestione:

- il "responsabile dell'area" ad accesso controllato che deve mantenere un effettivo controllo sull'area di sua responsabilità;
- la lista delle persone autorizzate ad accedere;
- la lista deve essere periodicamente controllata;
- i visitatori occasionali devono essere accompagnati;
- gli ingressi fuori orario devono essere controllati;
- deve essere assicurata l'esecuzione di periodici test sull'efficacia degli allarmi.

2.3 Rischio logico

Il rischio logico si riferisce all'utilizzo di elaboratori per la gestione degli archivi sia di dati comuni che sensibili. I rischi di questo tipo si possono così sintetizzare:

- rischio interno all'organizzazione relativo all'utilizzo della LAN/Intranet - Accesso alle banche dati da parte di personale, interno, non autorizzato causa mancanza di protezioni logiche a livello di software di sistema e/o applicativo;
- rischio esterno all'organizzazione - Accesso alle informazioni da parte di personale non autorizzato attraverso i punti di contatto con il mondo esterno Internet e RUPAR;
- rischio esterno dovuto ad intrusioni nel sistema da parte di hacker a fini dimostrativi o di sabotaggio;
- rischio interno/esterno di scaricamento virus e/o trojan per mezzo di posta elettronica e/o operazioni di download eseguite tramite il browser.
- rischio interno dovuto a intrusioni da parte di studenti;
- rischi interni ed esterni tipici dei servizi di rete che possono essere così riassunti:
 - **IP spoofing**- L'autore dell'attacco sostituisce la propria identità a quella di un utente legittimo del sistema. Viene fatto non per generare intrusione in senso stretto, ma per effettuare altri attacchi. Lo spoofing si manifesta come attività di "falsificazione" di alcuni dati telematici, come ad esempio di un indirizzo IP o dell'indirizzo di partenza dei messaggi di posta elettronica.
 - **Packet sniffing**- Apprendimento di informazioni e dati presenti sulla Rete o su un sistema, tramite appositi programmi. Consiste in un'operazione di intercettazione passiva delle comunicazioni di dati ed informazioni che transitano tra sistemi informatici. In particolare, un aggressore (attacker) può essere in grado di intercettare transazioni di varia natura (password, messaggi di posta elettronica etc.). L'intercettazione illecita avviene con l'ausilio degli sniffer, strumenti che catturano le informazioni in transito per il punto in cui sono installati. Gli sniffer possono anche essere installati su di un computer di un soggetto inconsapevole, in questo caso è possibile che prima dell'installazione dello sniffer, la macchina "obiettivo" sia stata oggetto di un precedente attacco e sia di fatto controllata dall'hacker.

- **Port scanning-** Serie programmata di tentativi di accesso diretti a evidenziare, in base alle “risposte” fornite dallo stesso sistema attaccato, le caratteristiche tecniche del medesimo (e le eventuali vulnerabilità), al fine di acquisire gli elementi per una “intrusione”. Trattasi di un vero e proprio studio delle vulnerabilità di un sistema; gli amministratori dei sistemi eseguono spesso questa funzione allo scopo di verificare la funzionalità del medesimo.
- **Highjacking-** Intrusione in una connessione di Rete in corso. In questo modo si colpiscono principalmente i flussi di dati che transitano nelle connessioni point to point. In sostanza l’hacker, simulando di essere un’altra macchina al fine di ottenere un accesso, si inserisce materialmente nella transazione, dopo averne osservato attentamente il flusso. L’operazione è complessa e richiede elevate capacità e rapidità d’azione.
- **Social engineering-** Apprendimento fraudolento da parte degli utenti di sistemi di informazioni riservate sulle modalità di accesso a quest’ultimo.
- **Buffer overflow-** Azioni che tendono a sfruttare eventuali anomalie e difetti di applicazioni che installate in alcuni sistemi operativi, forniscono le funzionalità di “amministratore del sistema”, consentendo il controllo totale della macchina. L’hacker, dunque, con tale azione va a sconvolgere la funzionalità di tali programmi, prendendo il controllo della macchina vittima;
- **Spamming-** Saturazione di risorse informatiche a seguito dell’invio di un elevato numero di comunicazioni tali da determinare l’interruzione del servizio. Ad esempio l’invio di molti messaggi di posta elettronica con allegati provoca, come minimo, la saturazione della casella e la conseguente non disponibilità a ricevere ulteriori (veri) messaggi.
- **Password cracking-** Sono programmi che servono per decodificare le password, una volta entrati in possesso del/dei file delle parole d’ordine.
- **Trojan-** Appartengono alla categoria dei virus, di solito sono nascosti in file apparentemente innocui che vengono inconsiamente attivati dall’utente. Permettono, una volta attivati, di accedere incondizionatamente al sistema.
- **Worm-** Appartengono alla categoria dei virus e sono programmi che si replicano attraverso i computer connessi alla rete. In genere consumano una gran quantità di risorse di rete (banda) e di conseguenza possono essere utilizzati per gli attacchi DOS (denial of service) in cui si saturano le risorse di un server o di una rete producendo una condizione di non disponibilità (non funzionamento).
- **Logic bomb-** Appartengono alla categoria dei virus e sono programmi che contengono al proprio interno una funzione diretta a danneggiare o impedire il funzionamento del sistema, in grado di attivarsi autonomamente a distanza di tempo dall’attivazione.
- **Malware e MMC (Malicious Mobile Code)-** Costituiscono la macrocategoria di codici avente come effetto il danneggiamento e l’alterazione del funzionamento di un sistema informativo e/o telematico. In tale categoria sono incluse anche alcune forme di codice ad alta diffusione, quali i virus, i worms ed i trojan horses.
- **DOS (Denial of Service)–** attacco che mira a saturare le risorse di un servizio,

di un server o di una rete.

- **DDOS (Distributed Denial of Service)**– attacco ripetuto e distribuito che mira a saturare le risorse di un servizio, di un server o di una rete

3. Misure minime di sicurezza adottate

Le misure minime di sicurezza adottate dall'istituto... si possono suddividere in due categorie:

- destinate ai supporti cartacei;
- destinate ai dati trattati in maniera informatica.

3.1 Archivi su supporto cartaceo

Le misure minime di sicurezza adottate per questo tipo di archivi sono così riassumibili.

3.1.1 Norme generali per tutti gli archivi su supporto cartaceo

Individuazione scritta di tutti gli incaricati del trattamento delle informazioni mediante l'uso del data base di cui al punto 2.1 del presente documento. Il data base deve essere costantemente aggiornato a cura del dirigente del servizio o suo incaricato;

- Accesso ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
- Utilizzo di archivi con accesso selezionato;
- Restituzione di atti e documenti al termine delle operazioni.

3.1.2 Norme per i dati sensibili e giudiziari

- Utilizzo di armadi o contenitori di sicurezza con chiave e caratteristiche ignifughe;
- controllo degli accessi agli archivi mediante l'utilizzo di apposito registro di carico e scarico dei documenti dall'archivio. Lo schema del registro è riportato nell'allegato D;
- identificazione e registrazione dei soggetti ammessi agli archivi dopo l'orario di chiusura.

3.2 Archivi su supporto informatico per elaboratori collegati su rete locale e geografica

Le misure minime di sicurezza adottate per questo tipo di archivi si riferiscono a dati sensibili e non in quanto si ritiene che le misure adottate, molte delle quali in uso da anni, tendono a dare la massima copertura sui rischi a prescindere dalla tipologia dei dati.

3.2.1 Sicurezza fisica dei calcolatori (descrizione dei server dell'istituto - sezione da personalizzare)

I Server Sissi e Docenti sono situati, unitamente al firewall e alle apparecchiature di telecomunicazioni in apposito locale adiacente a quelli destinati alla segreteria. Il locale è dotato di porta con serratura, normalmente chiusa, le chiavi sono custodite, in copia, dal dirigente scolastico, dal direttore dei servizi generali e amministrativi e dai responsabili del sistema informativo e del trattamento dei dati. L'alimentazione elettrica ai server ed alle apparecchiature di trasmissione è garantita da una linea elettrica privilegiata derivata direttamente dalla cabina di trasformazione e da un gruppo di continuità da 2.000 VA elettrici per un'autonomia a pieno carico di 15 minuti.

L'accesso al locale che ospita i server è vietato al personale non addetto alle operazioni di manutenzione, conduzione delle macchine (backup).

3.2.2 Difesa da accessi non autorizzati da rete geografica

La connettività internet è fornita tramite la rete RUPAR, per evitare l'accesso alla rete locale della segreteria da parte di utenti non autorizzati provenienti da RUPAR è stato installato un firewall di protezione che consente solo connessioni dall'interno verso l'esterno; eventuali operazioni di manutenzione al firewall non possono essere eseguite in remoto.

Il firewall è realizzato con tecnologia Open Source e sfrutta il kernel 2.4 di linux che consente l'utilizzo di un firewall di tipo "stateful packet-filtering"; la documentazione delle regole è conservata in busta chiusa nella cassaforte dell'istituto.

Il firewall svolge anche funzione di proxy e provvede all'aggiornamento del registro elettronico (file di log) delle richieste verso internet; i dati memorizzati sono:

- giorno/ora/minuto/secondo;
- indirizzo IP dell'PC che ha effettuato la richiesta;
- richiesta effettuata;
- codice della risposta dell'host remoto.

Tali dati possono essere utilizzati dal responsabile del sistema informativo per scopi statistici/funzionali.

La rete didattica è protetta da proprio firewall, realizzato con la stessa tecnologia del precedente; esso svolge funzioni di proxy e provvede all'aggiornamento del registro elettronico (file di log) con i seguenti dati:

- giorno/ora/minuto/secondo;
- indirizzo IP dell'PC che ha effettuato la richiesta;
- richiesta effettuata;
- codice della risposta dell'host remoto.

Tali dati possono essere utilizzati dal responsabile del sistema informativo e/o dai docenti responsabili dei laboratori per scopi statistici/funzionali.

Questo firewall svolge anche la funzione di filtro dei contenuti (vedere documento policy

di utilizzo della rete). Dal punto di vista tecnico il filtro (dansguardian) si posiziona tra le richieste dei browser e il proxy (squid), analizza, con algoritmi particolari, i contenuti delle pagine e ne autorizza/nega la visualizzazione.

Il filtro è altamente configurabile, la gestione della configurazione, che rispetta le indicazioni fornite dal Collegio dei Docenti, è responsabilità degli amministratori dei laboratori didattici.

Copia cartacea delle regole di configurazione del firewall del proxy e del filtro è conservata in cassaforte.

3.2.3 Codice identificativo degli utenti del sistema informativo

Tutti i Personal computer installati presso i locali della segreteria hanno la possibilità di attivare una password a livello di BIOS. Essendo il rapporto PC/posti di lavoro pari a 1 tutti gli utenti devono attivare una password di BIOS che renda esclusivo l'uso del personal computer al singolo operatore. Tale norma è obbligatoria per i posti di lavoro che contengono archivi di dati sensibili. In tal caso la gestione della password di BIOS è di esclusiva pertinenza del responsabile degli archivi. Non è consentita alcuna deroga. Il responsabile del trattamento provvederà ad istruire i responsabili degli archivi contenenti dati sensibili sulle modalità di inserimento e modifica delle password di BIOS.

Tutti gli utenti del software di segreteria Sissi accedono al sistema informativo per mezzo di user-id e password personale. User-id e password iniziale sono assegnati, in collaborazione con il responsabile del sistema informativo, in maniera univoca dal responsabile per il trattamento, che assegna inoltre le aree di competenza (p.es. alunni, bilancio, stipendi) e i diritti (lettura, scrittura). 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 6 caratteri di cui almeno uno deve essere rappresentato da numeri o caratteri speciali.

L'elenco degli user id e delle password è conservato in cassaforte.

Le password di amministratore o root di sistema di tutti i server sono inserite e modificate periodicamente dal responsabile del sistema informativo; sono conservate in busta chiusa nella cassaforte.

La password di root in caso di manutenzione straordinaria può essere affidata dal responsabile del sistema informativo al sistemista addetto alla manutenzione. In tal caso questa deve essere prontamente sostituita dal responsabile al termine delle operazioni di manutenzione a cui lo stesso deve sovrintendere.

Al momento della generazione della user-id all'utente viene assegnata una propria area disco, detta home, in cui può salvare i propri archivi.

Approfondimento sulle password

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.

Le regole di seguito elencate sono vincolanti per tutti i posti lavoro tramite i quali si può accedere alla rete e alle banche dati contenenti dati 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.

Devono essere rispettate le seguenti regole per la definizione/gestione delle password:

- la lunghezza minima della password è di 6 caratteri;
- deve contenere almeno un carattere alfabetico ed uno numerico;
- non deve contenere più di due caratteri identici consecutivi;
- non deve essere simile alla password precedente;
- non deve contenere l'user-id come parte della password;
- deve essere cambiata almeno ogni 6 mesi;
- non deve essere comunicata ad altri utenti.

Dove la tecnologia lo permette tali regole sono rese obbligatorie dal software altrimenti è responsabilità dell'utente rispettarle.

3.2.4 Protezione degli archivi informatici contenenti dati sensibili e giudiziari

Gli elaboratori che ospitano archivi con dati sensibili devono sottostare alle seguenti regole:

- Obbligo di password di BIOS;
- autorizzazione scritta per l'accesso agli incaricati ed agli addetti alla manutenzione;
- gli hard disk non devono essere condivisi in rete;
- supervisione dell'incaricato del trattamento a tutte le operazioni di manutenzione che devono essere effettuate on-site;
- antivirus costantemente aggiornato;
- piano di backup proceduralizzato concordato con i responsabili del trattamento e del sistema informativo;
- conservazione in armadio ignifugo e corazzato delle copie di backup;
- distruzione fisica dei floppy disk non utilizzati che contenevano copie parziali o totali degli archivi;
- obbligo di uso di screen saver con password;
- divieto di installazione, sui personal computer, di archivi con dati sensibili di carattere personale dell'utente;
- 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 che contengono archivi con dati sensibili accessi remoti di qualsiasi tipo mediante modem e linee telefoniche.

Il controllo dei documenti stampati è responsabilità degli incaricati al trattamento.

La stampa di documenti contenenti dati sensibili deve essere effettuata su stampanti poste in locali ad accesso controllato o presidiate dall'incaricato.

3.2.5 Salvataggio dei dati - Backup

Tutti gli utenti del sistema informativo, opportunamente istruiti, sono responsabili delle operazioni di salvataggio dei propri dati. Agli incaricati del trattamento dei dati sensibili Sig..... e Sig..... competono tutte le operazioni connesse al salvataggio giornaliero dei dati del sistema Sissi. Le operazioni di salvataggio avvengono tramite dispositivo DAT e consentono, oltre al salvataggio dei dati dell'applicativo Sissi anche quello delle home degli utenti. Pertanto l'uso da parte degli utenti delle home garantisce agli stessi un salvataggio quotidiano dei propri dati. Il salvataggio giornaliero si basa su 31 cassette DAT per cui i dati possono essere reperiti anche su serie storica legata ai giorni del mese. Ad ulteriore garanzia precisiamo che il server Sissi è dotato di controller RAID con mirroring (tre hard disk SCSI).

Le cassette sono conservate in cassaforte.

Per quanto riguarda il server docenti (linux) le copie vengono effettuate dai docenti incaricati professori..... con periodicità settimanale (4 cassette); il sistema prevede un raid software con due hard disk IDE. Le cassette sono conservate in armadio chiuso in sala docenti (chiavi disponibili solo agli incaricati).

Eventuali operazioni di restore devono essere supervisionate dal responsabile del sistema informativo o suo delegato.

I salvataggi che vengono di norma effettuati dagli utenti su floppy disk, e che quindi ricadono sotto la loro diretta responsabilità, devono essere conservati in più copie in appositi armadi in luoghi decentrati, per ovvi motivi di sicurezza, rispetto al posto di lavoro.

I responsabili del sistema informativo e del trattamento sconsigliano l'utilizzo dei floppy disk come supporto per le copie, a tal scopo sono stati installati sui pc della segreteria alcuni masterizzatori che permettono la copia su CD riscrivibili.

E' opportuno che gli utenti utilizzino la tecnica di trasferimento dei dati comuni sulla home in quanto ciò garantisce salvataggi quotidiani da parte degli incaricati. Per i dati sensibili le copie su floppy possono essere custodite in buste sigillate controfirmate sui lembi nella cassaforte.

3.2.6 La cassaforte

Nell'ufficio del Direttore dei servizi generali ed amministrativi si trova la cassaforte, in essa si trovano, oltre ad altri documenti le copie di backup dei dati informatici (cassette), copia delle password e degli user id, copia delle configurazioni del firewall, del proxy e del filtro dei contenuti, l'ufficio è dotato di serratura.

La chiave della cassaforte e dell'ufficio sono disponibili solo al Direttore dei servizi generali ed amministrativi e al Dirigente scolastico o suo delegato.

La scuola ha intenzione di dotarsi di un armadio ignifugo.

3.2.7 Protezione da Virus informatici

Su tutti i Personal computer degli utenti e sul server Sissi è installato apposito software antivirusin grado di prevenire attacchi di virus informatici. Detto software controlla anche le caselle di posta elettronica ed i file di attach. L'aggiornamento del software antivirus avviene settimanalmente attraverso internet.

L'utilizzo di software antivirus non è sufficiente da solo a garantire e prevenire attacchi di questo tipo. Appositi seminari sull'argomento garantiscono la cultura necessaria a far sì che gli utenti riducano al minimo i rischi prestando la massima attenzione allo scambio di dati con altri enti, nelle operazioni di FTP in rete e nei file attach di posta elettronica.

In considerazione dell'intesa MIUR - SUN Microsystem, che permetterà a docenti, studenti e personale ATA di disporre di una licenza gratuita di Staroffice, prevediamo di utilizzare tale sistema anche per ridurre il rischio virus derivante dalle macro che normalmente attaccano i file .doc di Microsoft Office.

Approfondimento sui virus

Le più recenti statistiche internazionali citano il virus informatico come minaccia più ricorrente ed efficace.

Secondo l'esperienza comune, un virus è riconducibile a un pezzo di codice eseguibile in grado di generare copie di se stesso (cioè di riprodursi) e di introdursi in file di dati e nel codice di altri programmi (cioè di infettare), provocando così effetti indesiderati, che vanno da semplici disturbi a conseguenze ben più gravi quali il danneggiamento di dati e/o la compromissione della funzionalità dell'intero sistema. L'introduzione di un virus può essere causata da un'operazione diretta quale il trasferimento di un file, la lettura di un e-mail (con allegato), l'installazione di una applicazione da un supporto esterno (floppy, CD, zip) o attraverso internet o con un'azione indiretta tra cui l'apertura di un file in formato Word o Excel (o tutti i formati che utilizzano un linguaggio eseguibile) contenente un macro virus o la visualizzazione di una pagina Web contenente un applet o un componente Activex.

I danni causati dai virus sono spesso agevolati dal fatto che l'utente utilizza il PC con pieno accesso a tutte le risorse del sistema, ovvero può installare programmi e accedere ai file importanti del sistema operativo in modalità scrittura (modificare/cancellare).

Il problema non è particolarmente grave nel caso di linux perché, come tutti i sistemi Unix le funzioni di amministratore di sistema (root) e di utente normale sono rigorosamente separate (i file di sistema importanti sono di proprietà dell'utente root, l'utente normale non vi ha accesso). La raccomandazione è quella di lavorare , in particolare quando connessi ad internet (navigare, scaricare email ecc.), come utente generico, in questo modo eventuali danni provocati da virus saranno limitati ai file a cui l'utente ha il permesso di accesso; lavorare invece come utente privilegiato, ovvero come root, abbassa il livello di sicurezza intrinseca del vostro sistema e permette, potenzialmente , ai virus di causare danni seri quali il danneggiamento dei file dell'utente e/o dell'ambiente di lavoro, costituito dal sistema operativo e dagli applicativi installati sul sistema.

Evidenziamo inoltre che sistemi operativi quali Windows 9x e Me non offrono una vera gestione della multiutenza e non permettono di imporre proprietà e diritti di accesso a file e directory; quindi da un punto di vista architetturale semplicemente non c'è nessuna protezione.

Prevediamo nell'anno solare 2004 la sostituzione, in segreteria, dei personal computer con sistemi operativi Windows 9x e Me.

3.2.8 Protezione da rischi durante la trasmissione dei dati

L'eventuale trasmissioni di dati ad altre amministrazioni quali Comuni, Provincia, Regione può avvenire solamente sulla rete RUPAR che garantisce criteri di riservatezza e confidenzialità.

3.2.9 Uso di programmi di sniffer e port scanning

E' vietato l'utilizzo di sniffer sulle reti dell'istituto e sul punto di accesso a RUPAR. L'uso di questo tipo di software è riservato esclusivamente al responsabile del sistema informativo suo delegato per la misura/diagnostica delle prestazioni di rete.

Non è ammessa in ogni caso la lettura in chiaro dei pacchetti in transito. Tale operazione deve essere autorizzata dalla Autorità Giudiziaria o dal Direttore scolastico per iscritto.

L'operazione di port scanning può essere eseguita dal personale sopraccitato per soli scopi diagnostici e solo all'interno della rete dell'istituto.

Nel caso degli studenti del corso di telecomunicazioni le operazioni citate hanno un alto valore didattico/professionale e di conseguenza possono essere eseguite su sistemi preparati allo scopo e con la indispensabile supervisione del docente responsabile del corso che concorda l'attività con il responsabile del laboratorio.

3.2.10 Riutilizzazione dei supporti di memorizzazione di dati sensibili

I supporti di memorizzazione di dati sensibili (hard disk, floppy disk, CD-ROM, dat, ecc.) sono soggetti alle seguenti misure di sicurezza:

- I floppy disk, CD-ROM, DAT non più utilizzati devono essere distrutti fisicamente mediante rottura delle parti principali e taglio delle superfici magnetiche (FD, DAT) alla presenza dell'incaricato del trattamento;
- Gli hard disk non più utilizzabili devono essere distrutti meccanicamente alla presenza dell'incaricato del trattamento;
- Gli hard disk ancora idonei all'uso, come nel caso di sostituzioni o dismissioni di personal computer, dovranno essere formattati a basso livello alla presenza dell'incaricato del trattamento che dovrà accertare, mediante apposito verbale, la reale cancellazione di tutti i dati con la collaborazione dell'Amministratore di Sistema;

4. Formazione

Il buon funzionamento di un piano di sicurezza si realizza attraverso il coinvolgimento di tutto il personale della scuola creando la cultura necessaria a garantire e a preservare l'integrità e la riservatezza dell'intero patrimonio informativo, con particolare attenzione ai dati sensibili.

La formazione continua, che deve coinvolgere tutto il personale di segreteria e docente,

si deve sviluppare attraverso le seguenti attività:

- Seminari di illustrazione del presente piano (destinatari tutti);
- Seminario sulla sicurezza destinato al personale di segreteria incaricato del trattamento dei dati sensibili;
- Seminario relativo all'uso consapevole della rete (destinatari docenti);
- Definizione dei contenuti ammessi (collegio docenti)
- Seminario con i responsabili delle varie attività, laboratori, copie ecc.
- Pubblicazione di normativa ed ordini di servizio in apposita bacheca situata in segreteria ed eventualmente in aula docenti.
- Destinazione di almeno il 20% del tempo di formazione nel settore informatica (corsi interni) ai temi della sicurezza e salvaguardia del patrimonio informativo della scuola (antivirus, backup, accessi controllati, ecc.).

5 Incident response informatico

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.

Tutti gli incaricati del trattamento dei dati sono pregati di avvisare tempestivamente i responsabili del sistema informativo e del trattamento 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 devono essere considerate le seguenti priorità:

- Evitare danni diretti alle persone;
- proteggere l'informazione sensibile o proprietaria;
- evitare danni economici;
- limitare i danni all'immagine dell'organizzazione.

Garantita l'incolumità fisica alle persone si può procedere a:

- isolare l'area contenente il sistema oggetto dell'incidente ;

- isolare il sistema compromesso dalla rete;
- spegnere correttamente il sistema (nel caso di sistemi windows staccare la presa dalla corrente);
- Documentare tutte le operazioni;

Una volta spento il sistema oggetto dell'incidente non deve più essere riacceso.

La successiva fase di indagine e di ripristino del sistema deve essere condotta da personale esperto di incident response, il dirigente scolastico e il responsabile del sistema informativo valuteranno se coinvolgere esperti e/o autorità competenti.

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 affrettato del sistema potrebbe alterare le prove dell'incidente.

6 Piano di attività annuale in tema di sicurezza

Al fine di aumentare i livelli di sicurezza nella protezione del patrimonio informativo della scuola è prevista la realizzazione nell'anno solare 2004 dei seguenti obiettivi:

- installazione di porte blindate per i locali contenenti dati sensibili e/o apparecchiature informatiche utilizzate per il trattamento dei dati;
- installazione di idonei armadi corazzati ed ignifughi per gli archivi cartacei contenenti dati sensibili e per le copie di backup;
- sperimentazione della trasmissione di dati in VPN con la sede coordinata di.....;
- adesione all'intesa MIUR/Sun microsystem per l'adozione del software "Staroffice" per ridurre il rischio di virus provenienti da macro di word;
- sostituzione dei computer e/o dei sistemi operativi Win9x e Me ancora presenti in segreteria con sistemi che gestiscano la multiutenza.

7 Aggiornamento del piano

Il presente piano è soggetto a revisione annua obbligatoria con scadenza entro il 31 dicembre. Il piano deve essere aggiornato ogni qualvolta si verificano le seguenti condizioni:

- modifiche all'assetto organizzativo della scuola ed in particolare del sistema informativo (sostituzioni di hardware, software, procedure, connessioni di reti, ecc.) tali da giustificare una revisione del piano;
- danneggiamento o attacchi al patrimonio informativo dell'ente tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

8 Allegati

- A) Schema funzionale delle connessioni dei server e delle reti geografiche;
- B) Schema RUPAR;
- C) Tracciato record del Data Base;
- D) Schema del registro dei movimenti dell'archivio cartaceo dei per dati sensibili;
- E) Modulo per l'archivio degli user id e delle password;

data,.....

Il responsabile del sistema informativo

Il responsabile del trattamento

Il Dirigente scolastico
