

Istituto professionale di Stato per L'Industria e l'Artigianato MORETTO
Via Apollonio, 21, BRESCIA

P R I V A C Y

(D.L.vo N. 196/2003)

QUARTA REVISIONE DELLE

DISPOSIZIONI MINIME SULLA SICUREZZA

E

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

**GIA' APPROVATO CON NOTA PROT.N. 601/A15 DEL
01.02.2005**

PRIMA REVISIONE PROT.N.2024/A15 DEL 6.4.2006

SECONDA REVISIONE PROT.N. 2085/A15 DEL 28.4.2007

TERZA REVISIONE PROT.N. 1606/A15 DEL 26.03.2008

Il presente documento si compone di n. 27 pagine (inclusa la presente)

**INTEGRAZIONE E RETTIFICA: DOCUMENTO E ALLEGATI N.1
E N.3**

Brescia, 30.03.2009

Prot. nr. 1550 /A15

**II TITOLARE DEL
TRATTAMENTO DEI DATI**

(Arturo Montanini)

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

STITUTO PROFESSIONALE DI STATO PER L'INDUSTRIA E L'ARTIGIANATO "MORETTO"

PREMESSA

Premesso che nell'ambito dell'attività dell'Istituto professionale di Stato per L'Industria e l'Artigianato MORETTO con sede in BRESCIA, Via Apollonio, 21, si effettuano trattamenti di dati personali, come di seguito elencati, il presente documento raccoglie e fornisce le informazioni utili per l'identificazione delle misure di sicurezza, organizzative, fisiche e logiche, previste per la tutela dei dati trattati.

Articolo 1

NORMATIVA DI RIFERIMENTO

- D.L.vo n. 196 del 30/06/2003;
- Regolamento per l'utilizzo della rete (all. 4)

Articolo 2

DEFINIZIONI E RESPONSABILITÀ

AMMINISTRATORE DI SISTEMA: il soggetto cui è conferito il compito di sovrintendere alle risorse del sistema operativo di un elaboratore o di un sistema di base dati e di consentirne l'utilizzazione. In questo contesto l'amministratore di sistema assume anche le funzioni di amministratore di rete, ovvero del soggetto che deve sovrintendere alle risorse di rete e di consentirne l'utilizzazione. L'amministratore deve essere un soggetto fornito di esperienza, capacità e affidabilità nella gestione delle reti locali.

Ai fini della sicurezza l'amministratore di sistema ha le responsabilità indicate nella lettera di incarico.

CUSTODE DELLE PASSWORD: il soggetto cui è conferito la gestione delle password degli incaricati del trattamento dei dati in conformità ai compiti indicati nella lettera di incarico.

DATI ANONIMI: i dati che in origine, o a seguito di trattamento, non possono essere associati a un interessato identificato o identificabile.

DATI PERSONALI: qualunque informazione relativa a persona fisica, persona giuridica, ente od associazione, identificati o identificabili, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

DATI IDENTIFICATIVI: i dati personali che permettono l'identificazione diretta dell'interessato.

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.

DATI GIUDIZIARI: i dati personali idonei a rivelare provvedimenti di cui all'articolo 3, comma 1, lettere da a) a o) e da r) a u), del D.P.R. 14 novembre 2002, n. 313, in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli articoli 60 e 61 del codice di procedura penale.

INCARICATO: il soggetto, nominato dal titolare o dal responsabile del trattamento, che tratta i dati. L'incaricato del trattamento dei dati, con specifico riferimento alla sicurezza, ha le responsabilità indicate nella lettera di incarico.

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. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

RESPONSABILE DELLA SICUREZZA INFORMATICA: il soggetto preposto dal titolare alla gestione della sicurezza informatica. 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. Ai fini della sicurezza il responsabile del sistema informativo ha le responsabilità indicate nella lettera di incarico.

TITOLARE: il titolare del trattamento è l'Ente (ISTITUTO SCOLASTICO) e la titolarità è esercitata dal rappresentante legale (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. Il titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

Articolo 3

TITOLARE, RESPONSABILI, INCARICATI

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

Titolare del trattamento : ARTURO MONTANINI
Amministratore della rete: FABIO PRANDELLI
Gestore della rete amministrativa: FABIO ODELLI
Gestore della rete di Istituto: LUCA DEL BARBA-FABIO PRANDELLI
Gestore delle passwords: LUCA DEL BARBA
Incaricati del trattamento dei dati: come da allegato 1
Incaricato dell'assistenza e della manutenzione degli strumenti elettronici: LUCA DEL BARBA-FABIO PRANDELLI

Articolo 4 ***ANALISI DEI RISCHI***

L'analisi dei rischi consente di acquisire consapevolezza e visibilità sul livello di esposizione al rischio del proprio patrimonio informativo e avere una mappa preliminare dell'insieme delle possibili contromisure di sicurezza da realizzare.

L'analisi dei rischi consiste nella:

- individuazione di tutte le risorse del patrimonio informativo;
- identificazione delle minacce a cui tali risorse sono sottoposte;
- identificazione delle vulnerabilità;
- definizione delle relative contromisure.

La classificazione dei dati in funzione dell'analisi dei rischi risulta la seguente:

- DATI ANONIMI, ovvero la classe di dati a minore rischio, per la quale non sono previste particolari misure di sicurezza;
- DATI PERSONALI,
 - DATI PERSONALI SEMPLICI, ovvero la classe di dati a rischio intermedio
 - DATI PERSONALI SENSIBILI/GIUDIZIARI, ovvero la classe di dati ad alto rischio;
 - DATI PERSONALI SANITARI, ovvero la classe di dati a rischio altissimo.

Articolo 5 ***INDIVIDUAZIONE DELLE RISORSE DA PROTEGGERE***

Le risorse da proteggere sono:

- personale;
- dati/informazioni;
- documenti cartacei;
- hardware;
- software;
- apparecchiature di comunicazione;
- servizi;

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

- immagine della scuola.

Per ulteriori dettagli vedere gli Allegati 1 e 3.

Articolo 6 **INDIVIDUAZIONE DELLE MINACCE**

Nella tabella seguente sono elencati gli eventi potenzialmente in grado di determinare danno a tutte o parte delle risorse indicate all'articolo 5.

Rischi	Deliberato	Accidentale	Ambientale
Terremoto			X
Inondazione	X	X	X
Uragano			X
Fulmine			X
Bombardamento	X	X	
Fuoco	X	X	
Uso di armi		X	
Danno volontario	X		
Interruzione di corrente		X	
Interruzione di acqua		X	
Interruzione di aria condizionata	X	X	
Guasto hardware		X	
Linea elettrica instabile		X	X
Temperatura e umidità eccessive			X
Polvere			X
Radiazioni elettromagnetiche		X	
Scariche elettrostatiche		X	
Furto	X		
Uso non autorizzato dei supporti di memoria	X		
Deterioramento dei supporti di memoria		X	
Errore del personale operativo		X	
Errore di manutenzione		X	
Masquerading dell'identificativo dell'utente	X		
Uso illegale di software	X	X	
Software dannoso		X	
Esportazione/importazione illegale di software	X		
Accesso non autorizzato alla rete	X		
Uso della rete in modo non autorizzato	X		
Guasto tecnico di provider di rete		X	
Danni sulle linee	X	X	
Errore di trasmissione		X	
Sovraccarico di traffico	X	X	
Intercettazione (Eavesdropping)	X		
Infiltrazione nelle comunicazioni	X		
Analisi del traffico		X	
Indirizzamento non corretto dei messaggi		X	
Reindirizzamento dei messaggi	X		
Ripudio	X		

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

Guasto dei servizi di comunicazione	X	X	
Mancanza di personale		X	
Errore dell'utente	X	X	
Uso non corretto delle risorse	X	X	
Guasto software	X	X	
Uso di software da parte di utenti non autorizzati	X	X	
Uso di software in situazioni non autorizzate	X	X	

Per ulteriori dettagli delle minacce relative all'aspetto informatico vedere l'Allegato 2

Articolo 7 **INDIVIDUAZIONE DELLE VULNERABILITÀ**

Nelle tabelle seguenti sono elencate le vulnerabilità del sistema informativo che possono essere potenzialmente sfruttate qualora si realizzasse una delle minacce indicate nell'articolo 6.

Infrastruttura	Hardware	Comunicazioni
Mancanza di protezione fisica dell'edificio (porte finestre ecc.)	Mancanza di sistemi di rimpiazzo	Linee di comunicazione non protette
Mancanza di controllo di accesso	Suscettibilità a variazioni di tensione	Giunzioni non protette
Linea elettrica instabile	Suscettibilità a variazioni di temperatura	Mancanza di autenticazione
Locazione suscettibile ad allagamenti	Suscettibilità a umidità, polvere, sporcizia	Trasmissione password in chiaro
	Suscettibilità a radiazioni elettromagnetiche	Mancanza di prova di ricezione/invio
	Manutenzione insufficiente	Presenza di linee dial-up (con modem)
	Carenze di controllo di configurazione (update/upgrade dei sistemi)	Traffico sensibile non protetto
		Gestione inadeguata della rete
		Connessioni a linea pubblica non protette

Documenti cartacei	Software	Personale
Locali documenti non protetti	Interfaccia uomo-macchina complicata	Mancanza di personale
Carenza di precauzioni nell'eliminazione	Mancanza di identificazione / autenticazione	Mancanza di supervisione degli esterni
Non controllo delle copie	Mancanza del registro delle attività (log)	Formazione insufficiente sulla sicurezza
	Errori noti del software	Mancanza di consapevolezza
	Tabelle di password non protette	Uso scorretto di hardware/software
	Carenza/Assenza di password management	Carenza di monitoraggio
	Scorretta allocazione dei diritti di accesso	Mancanza di politiche per i mezzi di comunicazione

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

	Carenza di controllo nel caricamento e uso di software	Procedure di reclutamento inadeguate
	Permanenza di sessioni aperte senza utente	
	Carenza di controllo di configurazione	
	Carenza di documentazione	
	Mancanza di copie di backup	
	Incuria nella dismissione di supporti riscrivibili	

Articolo 8 **INDIVIDUAZIONE DELLE CONTROMISURE**

Le contromisure individuano le azioni che si propongono al fine di annullare o di limitare le vulnerabilità e di contrastare le minacce, esse sono classificabili nelle seguenti tre categorie:

- contromisure di carattere fisico;
- contromisure di carattere procedurale;
- contromisure di carattere elettronico/informatico.

Contromisure di carattere fisico

- Le apparecchiature informatiche critiche (server di rete, computer utilizzati per il trattamento dei dati personali o sensibili/giudiziari e apparecchiature di telecomunicazione, dispositivi di copia) e gli archivi cartacei contenenti dati personali o sensibili/giudiziari sono situati in locali ad accesso controllato;
- i locali ad accesso controllato sono all'interno di aree sotto la responsabilità dell'Istituto IPSIA Moretto;
- i responsabili dei trattamenti indicati nell'allegato 1 sono anche responsabili dell'area in cui si trovano i trattamenti;
- i locali ad accesso controllato sono chiusi anche se presidiati, le chiavi sono custodite a cura di Maria Grazia Omelio(per cassaforte-) Angela Rossini(per locale server-cassaforte-)-Elena Panzera(per cassaforte e locale server di backup)-Daniela Lorica e Nino Cairone (per archivio posto nel seminterrato);
- l'ingresso ai locali ad accesso controllato è possibile solo dall'interno dell'area sotto la responsabilità dell'ISTITUTO ;
- i locali sono provvisti di sistema di allarme e di estintore
- i locali ad accesso controllato sono dotati di porte blindate, impianti elettrici dedicati,sistemi di condizionamento ove necessari , apparecchiature di continuità elettrica ove necessari. Sono programmati interventi per dotare i locali di armadi ignifughi

Contromisure di carattere procedurale

- l'ingresso nei locali ad accesso controllato è consentito solo alle persone autorizzate;
- il responsabile dell'area ad accesso controllato deve mantenere un effettivo controllo sull'area di sua responsabilità;
- nei locali ad accesso controllato è esposta una lista delle persone autorizzate ad accedere, che è periodicamente controllata dal titolare del trattamento o da suo delegato;
- i visitatori occasionali della aree ad accesso controllato sono accompagnati da

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

- un incaricato;
- per l'ingresso ai locali server è necessaria preventiva autorizzazione da parte del titolare del trattamento;
- è controllata l'attuazione del piano di verifica periodica sull'efficacia degli allarmi e degli estintori;
- l'ingresso in locali ad accesso controllato da parte di dipendenti o estranei per operazioni di pulizia o di manutenzione avviene solo se i contenitori dei dati sono chiusi a chiave e i computer sono spenti oppure se le operazioni si svolgono alla presenza dell'Incaricato del trattamento di tali dati;
- i registri di classe, contenenti dati comuni e particolari, durante l'orario delle lezioni devono essere tenuti in classe sulla scrivania e affidati all'insegnante di turno. Al termine delle lezioni vengono depositati dall'insegnante dell'ultima ora di lezione *in sala insegnanti, il cui accesso è riservato ai soli docenti e al personale incaricato della pulizia*;
- il docente è responsabile della riservatezza del registro personale in cui sono annotati dati comuni e particolari. Fuori dall'orario di servizio il registro viene conservato nell'armadietto del docente che è chiuso a chiave, una chiave di riserva è mantenuta *presso la segreteria di presidenza in un armadio chiuso a chiave*;
- il protocollo riservato, accessibile solo al Titolare del trattamento, è conservato *nell'ufficio di presidenza*;
- inoltre per il trattamento dei soli dati cartacei sono adottate le seguenti disposizioni:
 - si accede ai soli dati strettamente necessari allo svolgimento delle proprie mansioni;
 - si utilizzano archivi con accesso selezionato;
 - atti e documenti devono essere restituiti al termine delle operazioni;
 - è fatto divieto di fotocopiare/scannerizzare documenti senza l'autorizzazione del titolare del trattamento;
 - è fatto divieto di esportare documenti o copie dei medesimi all'esterno dell'Istituto professionale di Stato per L'Industria e l'Artigianato MORETTO, Via Apollonio, 21, BRESCIA senza l'autorizzazione del titolare del trattamento, tale divieto si estende anche all'esportazione telematica;
 - il materiale cartaceo asportato e destinato allo smaltimento dei rifiuti deve essere ridotto in minuti frammenti.

Contromisure di carattere elettronico/informatico

Vedere l'Allegato 3.

Articolo 9 NORME PER IL PERSONALE

Tutti i dipendenti concorrono alla realizzazione della sicurezza, pertanto devono proteggere le risorse loro assegnate per lo svolgimento dell'attività lavorativa e indicate nell'articolo 5, nel rispetto di quanto stabilito nel presente documento e dal regolamento di utilizzo della rete (Allegato 4).

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

Articolo 10 INCIDENT RESPONSE E RIPRISTINO

Vedere l'Allegato 3

Articolo 11 PIANO DI FORMAZIONE

La formazione degli incaricati viene effettuata all'ingresso in servizio, all'installazione di nuovi strumenti per il trattamento dei dati, e comunque con frequenza annuale. Le finalità della formazione sono:

- sensibilizzare gli incaricati sulle tematiche di sicurezza, in particolar modo sui rischi e sulle responsabilità che riguardano il trattamento dei dati personali;
- proporre buone pratiche di utilizzo sicuro della rete;
- riconoscere eventuali anomalie di funzionamento dei sistemi (hardware e software) correlate a problemi di sicurezza.

La formazione è stata fatta dal Prof. Giorgio Pedrazzi, docente di Informatica Giuridica presso l'Università Agli Studi di Brescia nel corso dell'anno 2004.

Nell'anno 2005/2006 l'Istituto ha aderito al corso di formazione organizzato dalla Direzione Regionale Lombardia in collaborazione con la Direzione Regionale del Friuli Venezia Giulia. Il corso ha avuto luogo presso L'Istituto ABBA-BALLINI di Brescia

Il piano prevede inoltre la pubblicazione di normativa ed ordini di servizio in apposita bacheca situata sulla parete di fronte all'ufficio della segreteria di presidenza

Articolo 12 AGGIORNAMENTO DEL PIANO

Il presente piano è soggetto a revisione annua obbligatoria con scadenza entro il 31 marzo, ai sensi dell'art. 19 allegato B del D.L.vo 30/06/2003 Num. 196. 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 della scuola tali da dover correggere ed aggiornare i livelli minimi di sicurezza previa analisi dell'evento e del rischio.

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

ELENCO ALLEGATI COSTITUENTI PARTE INTEGRANTE DI QUESTO DOCUMENTO

- Allegato 1 - elenco trattamenti dei dati
- Allegato 2 - minacce hardware, minacce rete, minacce dati trattati, minacce supporti
- Allegato 3 - misure di carattere elettronico/informatico, politiche di sicurezza, incident response e ripristino
- Allegato 4 - regolamento per l'utilizzo della rete
- Allegato 5 - uso del proxy
- Allegato 6 - attività di videosorveglianza
- Lettere di incarico per il trattamento dei dati
- Lettera di incarico per il custode delle password
- Lettera di incarico per l'amministratore di sistema
- Istruzioni operative per il gestore della rete di istituto
- Istruzioni operative per il gestore della rete amministrativa.
- Istruzioni per l'utilizzo della password
- Informativa per il trattamento dei dati delle aziende fornitrici e degli enti ed associazioni che hanno rapporti con la scuola
- Informativa per il trattamento dei dati del personale dipendente
- Informativa per il trattamento dei dati degli alunni e delle loro famiglie
- Istruzioni al personale amministrativo sulle modalità operative D.lgs 196/2003
- Istruzioni al personale tecnico sulle modalità operative D.Lgs 196/2003
- Modulo per l'esercizio di diritti in materia di protezione dei dati personali

Il presente Documento Programmatico sulla Sicurezza deve essere divulgato e illustrato a tutti gli incaricati.

Brescia, 30.03.2009

Il redattore del documento
(*Arturo Montanini*)

(firma)

Nota: Fonti di documentazione

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA

(ai sensi dell'art. 34 e regola 19 dell'Allegato B del Codice in materia di protezione dei dati personali del D.L.vo N. 196 del 30/06/2003)

Il modello di documento programmatico sulla sicurezza è stato predisposto consultando le seguenti fonti:

- <http://www.garanteprivacy.it>
- <http://www.osservatoriotecnologico.net>

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)

ALLEGATO 1 – Elenco trattamenti dei dati

Istituto professionale di Stato per L'Industria e l'Artigianato MORETTO
Via Apollonio, 21, BRESCIA

Tabella 1 - Elenco dei trattamenti dei dati

Dal riepilogo dei dati trattati e dall'identificazione degli strumenti utilizzati si delinea la seguente tabella:

Tipologia trattamento	Cartaceo	PC non in rete	PC in rete privata	PC in rete pubblica	Video Sorveglianza esterna
Dati comuni relativi a studenti e personale	X		X	X	
Dati comuni relativi a fornitori	X		X		
Dati comuni relativi ad altri soggetti			X		
Dati biometrici relativi a studenti/personale					
Dati idonei a rilevare la posizione di persone/oggetti	X		X	X	
Dati relativi allo svolgimento di at. econom./comm.	X		X		
Dati di natura giudiziaria	X				
Dati relativi al personale, candidati, anche sensibili	X		X		
Dati di natura anche sensibile relativi a clienti/utenti	X		X		
Dati idonei a rilevare lo stato di salute	X		X		

Analisi dei trattamenti effettuati

Dalla rilevazione degli strumenti utilizzati e delle tipologie di dati trattati emerge che:

- 1) solo i dati personali vengono trattati sistematicamente con supporti cartacei e con elaborazione;
- 2) i dati sensibili trattati con elaborazione, sono limitati a quelli strettamente necessari per assolvere gli obblighi normativi e contrattuali;
- 3) i dati giudiziari eventualmente trattati sono quelli necessari per assolvere agli obblighi normativi e di Legge, essi comunque non vengono trattati con elaborazione;

Descrizione sintetica del Trattamento		Natura dei dati trattati	Struttura di riferimento	Altre strutture che concorrono al trattamento	Descrizione degli strumenti utilizzati
Finalità perseguita o attività svolta	Categorie di interessati				
GESTIONE ALLIEVI	Allievi-famiglie	Anonimi-Semplici-sensibili-giudiziari-sanitari	Ufficio allievi-	Presidenza-staff dirigente-Segreteria di presidenza – docenti-ufficio contabilità – DSGA-coll.esterno fornitore del software di gestione allievi	P.C. collegati a rete locale e ad internet-armadi e schedari muniti di serratura-locale seminterrato adibito ad archivio.
GESTIONE DEL PERSONALE	Personale docente ed ATA in servizio o già in servizio nella scuola	Anonimi Semplici-sensibili-giudiziari-sanitari	Ufficio amministrazione del personale	Presidenza-staff dirigente Segreteria di presidenza - ufficio contabilità DSGA-ufficio allievi- fornitore esterno del software integrato per la gestione del	P.C. collegati a rete locale e ad internet-armadi e schedari muniti di serratura. locale seminterrato adibito ad archivio.

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)
ALLEGATO 1 – Elenco trattamenti dei dati

				personale	
GESTIONE DEI FORNITORI	Fornitori di beni e servizi	Anonimi- semplici- giudiziari	Uff. Acquisti/ ufficio tecnico	Presidenza- Segreteria allievi- segr.presidenza- uff.personale- uff.contabilità- magazzino-DSGA— fornitore esterno del software di gestione dei fornitori	P.C. collegati a rete locale e ad internet-armadi e schedari muniti di serratura. locale seminterrato adibito ad archivio.
GESTIONE COLLABORATORI ESTERNI	Collaboratori esterni	Anonimi- semplici- giudiziari	Ufficio contabilità	Presidenza- Segreteria allievi- segr.presidenza- uff.personale- uff.acquisti/uff.tecni co- DSGA- fornitore esterno del software integrato per la gestione del personale	P.C. collegati a rete locale e ad internet-armadi e schedari muniti di serratura. locale seminterrato adibito ad archivio.

**TIPOLOGIA DI DATI SENSIBILI E GIUDIZIALI TRATTATI ALL'INTERNO DELLE OPERAZIONI
INDISPENSABILI PER LA GESTIONE DEL SISTEMA ISTRUZIONE**

Di seguito si riportano le schede con l' indicazione delle singole attività, che prevedono il trattamento di dati sensibili

In questo trattamento tutti i dati sensibili sono trattati per le finalità di rilevante interesse pubblico di cui agli artt 68, 73, 86, 95 del D.lgs 30 giugno 2003, n.196

ATTIVITA' PROPEDEUTICHE ALL'AVVIO DELL'ANNO SCOLASTICO

I dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio.

Nell'espletamento di tale attività possono essere trattati i seguenti dati sensibili relativi:

alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana

alle convinzioni religiose, per garantire la libertà del credo religioso, l'insegnamento della religione cattolica o delle attività alternative.

Allo stato di salute, per assicurare l'erogazione del sostegno agli alunni diversamente abili e per la composizione della classi.

Alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione; i dati giudiziari emergono anche nel caso in cui l'Autorità giudiziaria abbia predisposto un programma di protezione nei confronti degli alunni nonché degli alunni che abbiamo commesso reati.

Fonti normative; Leggi regionali ai sensi DPR n.616/77-Legge 121/85- Legge 104/92 – D.lgs 297/94- Legge 196/97 – D.lgs 112/98- DPR 249/98- DPR 275/99- DPR 394/99- Legge 62/2000-Legge 53/2003- D.lgs 59/2004- D.lgs 76/2005- D.Lgs 226/2005.

I dati possono essere comunicati ai seguenti soggetti e per le seguenti finalità:

a) agli Enti Locali per la fornitura dei servizi ai sensi D.lgs 112/98 limitatamente ai dati indispensabili all'erogazione del servizio;

b) ai gestori pubblici e privati dei servizi di assistenza agli allievi e di supporto all'attività scolastica, ai sensi delle leggi regionali e in misura strettamente indispensabile per l'erogazione dei servizi;

c) alle ASL e agli enti locali per il funzionamento GLH e per la predisposizione e la verifica del PEI, ai sensi della legge 104/92

la raccolta dei dati può avvenire presso gli interessati o presso terzi e la loro elaborazione può avvenire in forma cartacea o con modalità informatizzate.

Altre operazioni ordinarie:registrazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, cancellazione e distruzione

TIPI DI DATI TRTTATI

ORIGINE X razziale X etnica

CONVINZIONI X religiose X altro genere

STATO DI SALUTE X patologie attuali e pregresse X terapie in corso X dati sulla salute relativi anche ai familiari

DATI CARATTERE GIUDIZIALE (art. 4, comma 1, lettera e), del Codice) X

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)
ALLEGATO 1 – Elenco trattamenti dei dati

In questo trattamento tutti i dati sensibili sono trattati per le finalità di rilevante interesse pubblico di cui agli artt 68, 73, 86, 95 del D.lgs 30 giugno 2003, n.196

ATTIVITA' EDUCATIVA, DIDATTICA E FORMATIVA, DI VALUTAZIONE

Nell'espletamento delle predette attività possono essere trattati dati sensibili relativi a:

alle origini razziali ed etniche, per favorire l'integrazione degli alunni con cittadinanza non italiana

alle convinzioni religiose, per garantire la libertà del credo religioso

Allo stato di salute, per assicurare l'erogazione del sostegno agli alunni diversamente abili, erogazione del servizio di mensa scolastica, all'insegnamento domiciliare ed ospedaliero, per la partecipazione alle attività educative e didattiche programmate, alle visite didattiche e di istruzione, alle attività sportive

Alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione

Alle convinzioni politiche per la formazione e funzionamento delle consulte e delle associazioni di studenti e famiglie.

I dati sensibili possono essere trattati per le attività di valutazione periodiche e finali, per le attività di orientamento e per la compilazione della certificazione delle competenze.

Fonti normative; Leggi regionali ai sensi DPR n.616/77-Legge 121/85- Legge 104/92 – D.lgs 297/94- DPR 567/96- Legge 196/97 – D.lgs 112/98- DPR 249/98- DPR 275/99- DPR 394/99- Legge 62/2000-Legge 53/2003- D.lgs 59/2004- D.lgs 76/2005- D.Lgs 226/2005.- DPR 301/2005

TIPI DI DATI TRATTATI

ORIGINE X razziale X etnica

CONVINZIONI X religiose X altro genere

STATO DI SALUTE X patologie attuali e pregresse X terapie in corso X dati sulla salute relativi anche ai familiari

DATI CARATTERE GIUDIZIALE (art.4,comma 1, lettera e), del Codice) X

I dati possono essere comunicati ai seguenti soggetti e per le seguenti finalità:

a) agli Enti Locali per la fornitura dei servizi ai sensi D.lgs 112/98 limitatamente ai dati indispensabili all'erogazione del servizio;

b) ai gestori pubblici e privati dei servizi di assistenza agli allievi e di supporto all'attività scolastica, ai sensi delle leggi regionali e in misura strettamente indispensabile per l'erogazione dei servizi;

c) alle altre istituzioni scolastiche, statali non statali per la trasmissione della documentazione relativa alla vita scolastica degli allievi, in misura strettamente indispensabile per l'erogazione dei servizi;

d) agli istituti di denuncia INAIL e alle agenzie di assicurazione infortuni e connessa responsabilità civile;

e) alle ASL e agli enti locali per il funzionamento GLH e per la predisposizione e la verifica del PEI, ai sensi della legge 104/92;

f) ad aziende, imprese ed altri soggetti pubblici e privati per tirocini formativi, stages e alternanza scuola-lavoro e, facoltativamente per finalità di rilevante interesse sociale ed economico, in misura strettamente indispensabile per l'erogazione dei servizi.

la raccolta dei dati può avvenire presso gli interessati o presso terzi e la loro elaborazione può avvenire in forma cartacea o con modalità informatizzate.

Altre operazioni ordinarie:registrazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, cancellazione e distruzione

In questo trattamento tutti i dati sensibili sono trattati per le finalità di rilevante interesse pubblico di cui agli artt 67, 71 del D.lgs 30 giugno 2003,196

RAPPORTI SCUOLA-FAMIGLIE: GESTIONE DEL CONTENZIOSO

Il trattamento di dati sensibili e giudiziari concerne tutte le operazioni connesse all'instaurazione di contenzioso con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio dell'istituto.

Fonti normative: Codice civile, codice penale, codice di procedura civile, codice di procedura penale, DPR 1199/71, D.lgs 297/94- DPR 249/98- DPR 275/99- Legge 53/2003- D.lgs 59/2004- D.lgs 76/2005 D.lgs 77/2005 D.lgs 226/2005

I dati possono essere comunicati ai seguenti soggetti e per le seguenti finalità:

Avvocatura dello Stato per la difesa erariali e consulenza presso gli organi di giustizia

Magistrature ordinarie e amministrativo-contabile e Organi di polizia giudiziaria, per l'esercizio dell'azione di giustizia
Liberi professionisti, ai fini di patrocinio o di consulenza, compresi quelli della controparte per le finalità di corrispondenza

la raccolta dei dati può avvenire presso gli interessati o presso terzi e la loro elaborazione può avvenire in forma cartacea o con modalità informatizzate.

Altre operazioni ordinarie:registrazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, cancellazione e distruzione

TIPI DI DATI TRATTATI

ORIGINE X razziale X etnica

CONVINZIONI X religiose X filosofiche X politiche X sindacali X altro genere

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)
ALLEGATO 1 – Elenco trattamenti dei dati

STATO DI SALUTE X patologie attuali e pregresse X terapie in corso X dati sulla salute relativi anche ai familiari
VITA SESSUALE X
DATI CARATTERE GIUDIZIALE (art.4,comma 1, lettera e), del Codice) X

In questo trattamento tutti i dati sensibili sono trattati per le finalità di rilevante interesse pubblico di cui agli artt 65 e 95 del D.lgs 30 giugno 2003,196

ORGANISMI COLLEGIALI E COMMISSIONI ISTITUZIONALI

Il trattamento dei dati sensibili è necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti nell'ordinamento scolastico.

Tali organismi sono rappresentativi sia del personale amministrativo e docente, sia delle famiglie, degli studenti e delle associazioni sindacali.

Il dato sensibile richiesto è quello dell'appartenenza sindacale, con riferimento agli organismi o comitati che richiedono la partecipazione di rappresentanti delle organizzazioni sindacali.

Fonti normative: D.lgs 297/94- CCNL, CCNI di comparto

TIPI DI DATI TRATTATI

CONVINZIONI

X Sindacali

DATI DI CARATTERE GIUDIZIARIO (art.4, comma 1, lettera e) del Codice) X

la raccolta dei dati può avvenire presso gli interessati o presso terzi e la loro elaborazione può avvenire in forma cartacea o con modalità informatizzate.

Altre operazioni ordinarie:registrazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, cancellazione e distruzione

In questo trattamento tutti i dati sensibili sono trattati per le finalità di rilevante interesse pubblico di cui agli artt 112, 62, 67, 68, 70, 72, 73 del D.lgs 30 giugno 2003,196

SELEZIONE E RECLUTAMENTO A TEMPO INDETERMINATO E DETERMINATO E GESTIONE DEL RAPPORTO DI LAVORO

- del personale in servizio o già in servizio nell'istituto

- dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello subordinato

1. i dati inerenti allo stato di salute sono trattati per : adozione di provvedimenti di stato giuridico ed economico, verifica dell'idoneità al servizio, assunzione del personale appartenente alle c.d. categorie protette, benefici previsti dalla normativa in tema di assunzioni, protezione della maternità, igiene e sicurezza sul luogo di lavoro, causa di servizio, equo indennizzo, onorificenze, svolgimento di pratiche assicurative, previdenziali e pensionistiche obbligatorie e contrattuali, trattamenti assistenziali, riscatti e ricongiunzioni previdenziali, denunce di infortuni e/o sinistri e malattie professionali, fruizione di assenze, particolari esenzioni o permessi lavorativi collegati a particolari condizioni di salute dell'interessato o dei suoi familiari, assistenza fiscale, mobilità territoriale, professionale e intercompartimentale;

2. i dati idonei a rilevare l'adesione a sindacati o organizzazioni di carattere sindacale per gli adempimenti connessi al versamento delle quote di iscrizione o per l'esercizio dei diritti sindacali;

3. I dati sulle convinzioni religiose per la concessione dei permessi per festività oggetto di specifica richiesta dell'interessato motivata per ragioni di appartenenza a determinate confessioni religiose. I dati sulle convinzioni religiose vengono in rilievo anche per il reclutamento dei docenti di religione;

4. I dati sulle convinzioni filosofiche o d'altro genere possono venire in evidenza dalla documentazione connessa allo svolgimento del servizio di leva come obiettore di coscienza;

5. I dati di carattere giudiziario sono trattati nell'ambito delle procedure concorsuali al fine di valutare il possesso dei requisiti di ammissione e per l'adozione dei provvedimenti amministrativo contabili connessi a vicende giudiziarie che coinvolgono l'interessato;

6. Le informazioni di carattere sessuale possono desumersi unicamente in caso di eventuale rettificazione di attribuzione di sesso.

Fonti normative: DPR n.3/57- legge 104/92- legge 68/99- D.lgs 165/2001- legge 145/2002- R.D. 1290/22- legge 336/70- legge 1204/71- DPR 1032/73- DPR 1092/73- legge 29/79- legge 45/90- D.lgs 503/92- legge 20/94- legge 335/95- legge 38/98- legge 68/99- D.P.C.M. 20 dicembre 1999- legge 53/2000- DPR 461/2001- D.lgs 297/94- Legge 124/99- legge 186/2003- D.lgs 59/2004- legge 143/2004- CCNL e CCNI del comparto scuola e della separata AREA DELLA Dirigenza scolastica, legge 37/90- legge 448/98- DPR 190/2001- legge 289/2002- D.lgs 227/2005.

TIPI DI DATI TRATTATI

CONVINZIONI X religiose X filosofiche X altro genere X sindacali

STATO DI SALUTE X patologie attuali e pregresse X terapie in corso X dati sulla salute relativi anche ai familiari

VITA SESSUALE X (solo in caso di rettificazione di attribuzione di sesso)

DATI DI CARATTERE GIUDIZIARIO (art.4, comma 1, lettera e) del Codice) X

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)
ALLEGATO 1 – Elenco trattamenti dei dati

Particolari forme di trattamento:

interconnessione e raffronto di dati con altro titolare: amministrazioni certificanti in sede di controllo delle dichiarazioni sostitutive ai fini del DPR 445/2000

Comunicazione ai seguenti soggetti per le seguenti finalità:

- servizi sanitari competenti per visite fiscali e per l'accertamento dell'idoneità all'impiego;
- organi preposti al riconoscimento della causa di servizio/equo indennizzo, ai sensi del DPR 461/2001;
- Organi preposti alla vigilanza in materia di sicurezza e di igiene sui luoghi di lavoro(D.lgs 626/94);
- Enti assistenziali, previdenziali e assicurativi, autorità di pubblica sicurezza ai fini assistenziali e previdenziali, nonché per la denuncia di malattie professionali o infortuni sul lavoro ai sensi del DPR 1124/65;
- Amministrazioni provinciali per il personale assunto obbligatoriamente ai sensi della legge 68/1999;
- Organizzazioni sindacali per gli adempimenti connessi al versamento delle quote di iscrizione e per la gestione dei permessi sindacali;
- Pubbliche Amministrazioni presso le quali vengono comandati i dipendenti, o assegnati nell'ambito della mobilità;
- Ordinario Diocesano per il rilascio dell'idoneità all'insegnamento della Religione cattolica ai sensi della legge 186/2003;
- organi di controllo ai fini del controllo di legittimità e annotazione della spesa dei provvedimenti di stato giuridico ed economico del personale ex legge 20/94 e DPR 38/98;
- Agenzia delle Entrate ai fini degli obblighi fiscali del personale ex legge 413/91;
- MEF e INPDAP per la corresponsione degli emolumenti connessi alla cessazione del servizio ex legge 335/95;
- USP per la rilevazione annuale dei permessi per cariche sindacali e funzioni pubbliche elettive.

la raccolta dei dati può avvenire presso gli interessati o presso terzi e la loro elaborazione può avvenire in forma cartacea o con modalità informatizzate.

Altre operazioni ordinarie:registrazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, cancellazione e distruzione

In questo trattamento tutti i dati sensibili sono trattati per le finalità di rilevante interesse pubblico di cui agli artt 112, 67, 71 del D.lgs 30 giugno 2003,196

GESTIONE DEL CONTENZIOSO E PROCEDIMENTI DISCIPLINARI

Il trattamento dei dati sensibili e giudiziari concerne tutte le attività relative alla difesa in giudizio dell'Istituto e del Ministero della Pubblica Istruzione nel contenzioso del lavoro amministrativo, nonché quelle connesse alla gestione degli affari penali e civili.

Fonti normative

Codice civile e penale, Codice procedura civile e penale, DPR 3/57, DPR 1199/71, Legge 1034/71, legge 59/97, Legge 205/2000, D.lgs 274/2000, legge 97/2001, D.lgs 165/2001, Accordi quadro, D.lgs 297/94, DPR 190/2001, CCNL e CCNI del comparto scuola e della separata area della Dirigenza scolastica.

TIPI DI DATI TRATTATI

ORIGINE X razziale X etnica

CONVINZIONI X religiose X filosofiche X altro genere X sindacali X politiche

STATO DI SALUTE X patologie attuali e pregresse X terapie in corso X dati sulla salute relativi anche ai familiari

VITA SESSUALE X

DATI DI CARATTERE GIUDIZIARIO (art.4, comma 1, lettera e) del Codice) X

Particolari forme di trattamento:

- Ministero del Lavoro e delle Politiche Sociali per lo svolgimento dei tentativi obbligatori di conciliazione dinanzi ai Collegi di conciliazione ex D.lgs 165/2001
- Organi arbitrali per lo svolgimento delle procedure arbitrali ai sensi del CCNL del settore;
- Avvocatura dello Stato per la difesa erariale e consulenza presso gli Organi di giustizia;
- magistrature ordinarie ed amministrative-contabili e organi di polizia giudiziaria per l'esercizio dell'azione di giustizia;
- liberi professionisti ai fini di patrocinio o di consulenza, compresi quelli di controparte per le finalità di corrispondenza sia in fase giudiziale che stragiudiziale.

la raccolta dei dati può avvenire presso gli interessati o presso terzi e la loro elaborazione può avvenire in forma cartacea o con modalità informatizzate.

Altre operazioni ordinarie:registrazione, conservazione, consultazione, modificazione, selezione, estrazione, utilizzo, cancellazione e distruzione

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)
ALLEGATO 1 – Elenco trattamenti dei dati

Tabella 2 - Descrizione della struttura organizzativa dell'Istituto professionale di Stato per L'Industria e l'Artigianato MORETTO, Via Apollonio, 21, BRESCIA

Struttura	Trattamenti effettuati dalla struttura	Descrizione dei compiti e delle responsabilità della struttura
UFFICIO DEL DIRETTORE SERVIZI GENERALI E AMMINISTRATIVI	Garantisce l'unitarietà dell'organizzazione dei servizi amministrativi, tecnici e ausiliari dell'istituto in coerenza con il POF e le direttive del dirigente scolastico. Garantisce l'esercizio del diritto di informazione, di accesso e di partecipazione assicurati dalla legge sulla trasparenza amministrativa. Assicura la reciproca informazione tra gli uffici interni e con le altre strutture operanti nell'amministrazione scolastica, nonché fra gli uffici per le relazioni con il pubblico delle altre amministrazioni.	Consultazione e trattamento di tutti i dati, sia in formato cartaceo che in Formato elettronico, depositati nell'istituto, al fine di garantire: <ol style="list-style-type: none"> 1. l'unitarietà dell'organizzazione dei servizi amministrativi, tecnici ed ausiliari ; 2. il diritto all'accesso di terzi, titolari di interessi, ai dati depositati nell'istituto; 3. comunicazione a terzi nei casi previsti da specifiche norme di legge.
STAFF DI DIRIGENZA	Collabora con il dirigente scolastico, titolare del trattamento, nella gestione del personale docente, ATA e degli allievi	Consultazione e trattamento di tutti i dati, relativi al personale ed agli allievi, al fine di garantire il regolare funzionamento dell'Istituto e l'assolvimento di obblighi di legge.
SEGRETERIA ALLIEVI	Gestione carriera scolastica degli allievi Attività propedeutiche inizio anno scolastico Pratiche infortuni allievi e personale interno-gestione protocollo in uscita	Acquisizione e caricamento dei dati relativi ad allievi e famiglie per la gestione della carriera scolastica degli allievi e per corresponsione di eventuali benefici economici previsti da norme di legge. Acquisizione cartacea dei dati necessari alla gestione degli infortuni. Consultazione. Comunicazione a terzi nei casi previsti da specifiche norme di legge.
SEGRETERIA DI PRESIDENZA	Gestione organico docente ed ata- Gestione supplenze interne docenti- Gestione scioperi ed assemblee sindacali-gestione cartellino delle presenze- gestione protocollo in uscita	Acquisizione e caricamento dei dati relativi ai docenti e al personale ATA per la gestione delle supplenze interne e partecipazione a scioperi e assemblee sindacali. Acquisizione cartacea nel fascicolo personale degli stessi. Consultazione. Comunicazione a terzi nei casi previsti da specifiche norme di legge.
UFFICIO AMMINISTRAZIONE DEL PERSONALE	Gestione stato giuridico del personale docente ed ATA a tempo determinato ed indeterminato. Gestione protocollo.	Acquisizione e caricamento dei dati relativi a tutto il personale in servizio ai fini della gestione dello stato giuridico ed economico dello stesso. Acquisizione cartacea degli stessi dati nel fascicolo personale dell'interessato. Consultazione. Comunicazione a terzi nei casi previsti da specifiche norme di legge.
UFFICIO CONTABILITA'	Gestione dello stato economico del personale docente ed ATA-Gestione dei fornitori di beni e servizi e dei collaboratori esterni- gestione protocollo in uscita	Acquisizione e caricamento dei dati relativi a tutto il personale in servizio ai fini della gestione dello stato economico dello stesso. Acquisizione cartacea degli stessi dati nel fascicolo

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)
ALLEGATO 1 – Elenco trattamenti dei dati

		personale dell'interessato. Consultazione. Comunicazione a terzi nei casi previsti da specifiche norme di legge.
UFFICIO ACQUISTI E DEL PATRIMONIO/UFFICIO TECNICO	Predisposizione attività istruttoria ai fini dell'acquisizione di beni e servizi-gestione protocollo in uscita	Acquisizione e caricamento dei dati relativi a tutti i fornitori di beni e servizi. Acquisizione cartacea degli stessi dati nell'archivio dell'istituto. Consultazione .Comunicazione a terzi nei casi previsti da specifiche norme di legge.
UFFICIO MAGAZZINO	Controllo, carico nel magazzino e distribuzione al personale del materiale acquistato- gestione protocollo in uscita	Acquisizione e caricamento dei dati relativi a tutti i fornitori di beni e servizi.Acquisizione cartacea degli stessi dati nell'archivio dell'Istituto.Consultazione.Comunicazione a terzi nei casi previsti da specifiche norme di legge.
GRUPPO RETE	Manutenzione di tutte le strutture informatiche,ad uso amministrativo e didattico, presenti in Istituto. Gestione del sito web (Golem) dell'istituto.Gestione del server di posta interna.Gestione password utenti autorizzati.	Accesso a tutti i dati elettronici relativi ad allievi,famiglie, personale, fornitori, collaboratori esterni, ai soli fini di manutenzione e di backup.

Tabella 3 – Elenco del personale incaricato del trattamento in ogni struttura e delle dotazioni informatiche.

Nome e cognome	Struttura di riferimento	Strumenti utilizzati	Responsabilità aggiuntive
Cairone Antonino	Segreteria Allievi	Vedi tabella 2 dell'allegato 3	custode chiavi armadi segreteria allievi-custode propria password personale-utilizzo fax
Lorica Daniela	Segreteria Allievi	Vedi tabella 2 dell'allegato 3	custode chiavi armadi segreteria allievi- custode propria password personale-utilizzo fax
Panzerà Elena	Ufficio acquisti e del patrimonio/ufficio tecnico	Vedi tabella 2 dell'allegato 3	Custode chiavi armadi siti nell'ufficio-custode chiavi cassaforte sita nell'ufficio del DSGA.- custode propria password personale-utilizzo fax
Rizzuto Antonino	Ufficio acquisti e del patrimonio/ufficio tecnico	Vedi tabella 2 dell'allegato 3	custode chiavi ufficio tecnico- custode propria password personale-utilizzo fax
Losco Lia	Ufficio amministrazione del personale	Vedi tabella 2 dell'allegato 3	Custode chiavi armadi siti nell'ufficio- custode propria password personale-utilizzo fax
Nesi Pino	Ufficio contabilità	Vedi tabella 2 dell'allegato 3	Custode chiavi armadi siti nell'ufficio- custode propria password personale-utilizzo fax
Omelio Maria Grazia	Ufficio DSGA	Vedi tabella 2 dell'allegato 3	Custode chiavi cassaforte e proprio ufficio-custode chiavi locale del server di backup.- custode propria password personale-

Documento programmatico sulla sicurezza (ai sensi del D.L.vo n. 196 del 30/06/03)
ALLEGATO 1 – Elenco trattamenti dei dati

			utilizzo fax
Fragapane Maria Giuseppa	Ufficio amministrazione del personale	Vedi tabella 2 dell'allegato 3	Custode chiavi armadi siti nell'ufficio- custode propria password personale-utilizzo fax
Rossini Angela	Ufficio di presidenza	Vedi tabella 2 dell'allegato 3	Custode chiavi armadi siti nell'ufficio-custode chiavi cassaforte e ufficio DSGA- custode chiavi armadi presidenza.- custode propria password personale-utilizzo fax
Delbarba Luca	Gruppo rete		Gestione sito Web "Golem" -custode delle password.- custode propria password personale- Gestione server rete didattica
Prandelli Fabio	Gruppo rete		Gestione sito Web "Golem" – amministratore di posta elettronica-custode delle password.- custode propria password personale- Gestione server rete didattica
Odelli Fabio	Gruppo rete		Gestione server amministrazione (SISSI).- custode propria password personale
Antonio Arcangelo	Staff dirigenza	Vedi tabella 2 dell'allegato 3	Custode chiavi vice presidenza-custode propria password personale

SERVIZIO DI POSTA ELETTRONICA

Il servizio di posta elettronica per i servizi amministrativi sul dominio ipsiamoretto.it è gestito da GMAIL (servizio di posta di Google).

Amministratore del servizio è il Prof. Fabio Prandelli

Gli assistenti amministrativi sono titolari di casella di posta elettronica personale, mentre ciascun ufficio ha un indirizzo di posta elettronica "istituzionale" su cui confluiscono le e-mail riguardanti gli uffici.

Il sistema in automatico smista le e-mail istituzionali in arrivo e in partenza dalle caselle degli uffici sulle caselle personali dei componenti dei rispettivi uffici, alla casella del dirigente scolastico e alla casella del DSGA. Non è previsto il percorso inverso, pertanto le e-mail in partenza ed in arrivo dalle caselle personali restano nelle stesse e non sono visibili sulle caselle "istituzionali".

Brescia, 30.03.2009

IL TITOLARE DEL TRATTAMENTO
 (Arturo Montanini)

Nota: parte delle indicazioni sono tratte dalla "Guida operativa per redigere il documento programmatico sulla sicurezza (DPS)" pubblicate dal garante

**Istituto professionale di Stato per L'Industria e l'Artigianato
MORETTO
Via Apollonio, 21, BRESCIA**

Tabella 1 – RETE TELEMATICA

Il sistema di lavoro della struttura avviene con elaborazione in rete INTRANET protetta da Firewall. Si dispone di una rete, realizzata mediante collegamenti via cavo costituita da:

- n 4 server, così identificati:
 - nell'ufficio contabilità (dati del personale)
 - nella sala macchine server Moretto web
 - nella sala macchine server Proxy Censornet

- n 15 postazioni lavoro dislocate nei vari uffici dell'amministrazione
- n 10 stampanti di cui n 1 laser in rete dislocate nell'area ufficio
- n 1 fax localizzato nell'area ufficio segreteria di presidenza
- n 1 dispositivo di backup localizzato nell'area ufficio contabilità

NB.: I server attualmente in funzione sono i seguenti :

- a) Moretto: Fisicamente collocato nell'ufficio contabilità corredato di sistema operativo Windows 2003 Server con Firewall integrato. Sul medesimo server sono registrate sia le informazioni sensibili riguardanti gli allievi (Archivi Gemma) sia quelle riguardanti il personale (Archivi Sissi e protocollo informatico).
- b) Didattica: Fisicamente collocato nel locale server, corredato di sistema operativo Windows 2003 Server con Firewall integrato funziona da server Web di Istituto sia sulla rete interna (Intranet di Istituto) che sulla rete pubblica (Internet) (www.ipsiamoretto.it). Sul server Didattica sono disponibili aree-dati di condivisione per la memorizzazione di esercitazioni di laboratorio dei diversi settori in cui si articolano gli insegnamenti del nostro istituto.
- c) Proxy Censornet: Fisicamente collocato nel locale server, corredato di sistema operativo Linux svolge le funzioni di proxy per gli accessi a Internet dalla rete Didattica. Registra i parametri di navigazione di tutti gli Studenti, dei Docenti e dei Tecnici di Laboratorio conformemente alle disposizioni relative alla "tracciabilità". Nega la navigazione su "siti web" definiti in "blacklist" e a quelli che contengono frasi/parole e combinazioni relative a pornografia e violenza, consente la navigazione su "siti web" definiti in "whitelist".
- d) Il vecchio server della rete Amministrativa, su di esso sono tuttora attivi due servizi residui (Win-Tax tariffazione telefonate e VisualTime registrazione accesso cartellini).

D - Elaboratori in rete pubblica

Sono dotati di un accesso ad internet da parte di utenti autorizzati circa 120 PC all'interno dell'istituto. L'autorizzazione è verificata tramite un sistema di autenticazione dell'accesso.

Connettività	Apparecchiature di comunicazione	Provider
ADSL 4 M bit/s	Router adsl Netgear	interbusiness

Modalità di accesso ad Internet nella scuola:

La navigazione in Internet avviene attraverso un sistema di *autenticazione* e di *filtro dei contenuti*. Il sistema in oggetto è sostanzialmente un proxy basato sul sistema operativo linux. Chiamiamo per comodità tale sistema "*Proxy Censornet*".

Autenticazione:

Tutti gli utenti abilitati alla navigazione sono forniti di un “Codice Utente” e di una “Password”.

Il “Codice Utente” è un numero univoco di 12 cifre generato sulla base del cognome, nome, data di nascita e gruppo di appartenenza dell’utente (per gli studenti il gruppo è la classe).

La 1° password di accesso viene generata in modalità casuale combinando un numero di 4 cifre ed un nome proprio (es. 8745Gustavo, 1371Eugenio).

La password potrà essere modificata direttamente dall’utente attraverso un programma dedicato installato nei laboratori di informatica info 1 e info 2 sul PC del tecnico di laboratorio.

Ogni accesso ad internet viene registrato in maniera anonima dal sistema “*Proxy Censornet*”.

Solo l’amministratore può tracciare la navigazione effettuata dagli utenti noto il loro codice utente (univocamente definito da cognome, nome e data di nascita dell’utente).

Gli utenti abilitati all’accesso ad internet sono stati suddivisi nelle seguenti categorie:

- 1- Amministratori
- 2- Docenti
- 3- ATA
- 4- Amministrativi
- 5- Studenti

Le liste aggiornate degli utenti sono fornite da un programma dedicato (creato dal prof. Azzani) che si occupa di interrogare il database del programma SISSI che contiene i dati aggiornati di tutto il personale della scuola e degli studenti.

Tali liste di utenti vengono utilizzate da un altro programma (creato dal prof. Delbarba) per creare i “codice utenti” e la prima “password” di accesso ad internet.

Filtro dei Contenuti:

Il sistema “*Proxy Censornet*” impedisce agli utenti:

- la navigazione senza il codice utente e la password
- la navigazione su siti pornografici
- la navigazione su siti di violenza
- la navigazione su siti indicati dagli amministratori
- lo scaricamento di programmi non consentiti (musica, video, ecc..)
- l’esecuzione di programmi di accesso ad internet diversi dal Browser (http)

Registrazione degli accessi

Il sistema *ProxyCensornet* registra tutti gli accessi ad internet effettuati dagli utenti e li mantiene nel proprio database per un tempo pari a 2 mesi.

Trascorsi 2 mesi dalla data odierna gli accessi registrati vengono eliminati.

Nota tecnica: ricerca e test del sistema da utilizzare per permettere l’accesso sicuro ad Internet

Sono stati testati una decina di prodotti open source e/o commerciali.

Alla fine la scelta è caduta su una soluzione open source (inglese → www.censornet.com) basata sul sistema operativo linux molto utilizzata in ambito scolastico e accademico.

Programma per il cambio della password

L’utente deve essere in grado di modificare la propria password in modo che la responsabilità di eventuali abusi sia completamente a suo carico.

Solo l’amministratore del sistema può risalire alla password dell’utente a partire dal suo codice.

Sistema per la registrazione degli accessi ad internet per 30 mesi

La normativa attuale prevede la registrazione degli accessi ad internet per 30 mesi.

Il sistema “ProxyMoretto” salva i dati solo per 2 mesi.

È stato creato da Delbarba un programma che giornalmente salva i dati giornalieri del proxy Censornet in un database installato sul server Moretto Web (soggetto a backup esterno) in modo da estendere il periodo di registrazione da 2 a 30 mesi.

Programma per l'abilitazione dei PC alla navigazione internet

Per impedire un abuso dell'accesso ad Internet da parte degli utenti è stato creato da Delbarba un programma che permette di disabilitare l'accesso ad Internet da parte di tutti i PC di uno specifico laboratorio o di un singolo PC. Il programma è installato sul PC del tecnico di laboratorio ed è accessibile solo in modalità di amministratore del PC.

L'abilitazione all'accesso ad internet viene di norma effettuata solo su richiesta da parte dei docenti che accedono ai laboratori per finalità didattiche.

Attività ANCORA DA EFFETTUARE:

1- Automatizzare il programma di gestione degli utenti

Il programma dovrà mantenere aggiornata *in automatico* la lista degli utenti presenti nel sistema "ProxyCensornet" sulla base delle liste utenti generate dal programma creato da Delbarba. Gli utenti dovranno essere mantenuti in archivio per 30 mesi.

Tabella 2 - Descrizione Personal Computer

	UBICAZIONE	UTENTE	CPU	MHZ	RAMT	IP	SOFTWARE	SO
1	AMMINISTRAZIONE	Pino Nesi	Athlon XP	1250	512	192.168.146.3	1-2-11	W2K
2	AMMINISTRAZIONE	Panzerà	C. Duo E5200	2500	2000	192.168.146.92	1-2-11-10-4-3-9	WXP
3	DSGA	Omelio	Pentium IV	3000	512	192.168.146.26	1-2-3-4-11-13-9-10-5	WXP
4	MAGAZZINO	Fragapane	Athlon XP	1660	512	192.168.146.39	1-3	W2K
5	UFFICIO TECNICO	Azzani	Sempron	1533	512	192.168.146.31	1-3-4-6-	WXP
6	PRESIDENZA	Montanini	Pentium IV	3000	512	192.168.146.13	1-14	WXP
7	SEGR. PRESIDENZ	Rossini	Sempron 3000	1816	512	192.168.146.16	1-2-5-6-11-12-13	WXP
8	UFF. ALLIEVI	Cairone	Athlon XP	1250	512	192.168.146.17	1-2-7-11-14	W2K
9	UFF. ALLIEVI	Lorica	Athlon	1533	512	192.168.146.18	1-2-7-11-14	WXP
10	UFF. ALLIEVI	Lorica	C. Duo E5200	2500	2000	192.168.146.28	1-2-7-11-14	W2k
11	UFF. PERSONALE	Pezzato-Losco	Athlon XP	1250	512	192.168.146.10	1-2-11	W2K
12	UFF. PERSONALE	Losco	Athlon XP 64	1000	512	192.168.146.12	1-2-5-11	W2K
13	UFF. PERSONALE	Pezzuto	AMD Athlon	1766	512	192.168.146.9	1-2-11	W2K
14	UFF. TECNICO	Rizzuto	AMD Athlon	1800	512	192.168.146.33	1-6	W2K
15	V.PRESIDENZA	Arcangelo	Athlon	1800	512	192.168.146.24	1-6	W2K

SOFTWARE INSTALLATO

		PRODUTTORE
1	Office	MICROSOFT
2	Sissi in Rete	MIUR
3	Magazzino2004	INTERNA AZZANI
4	Biblioteca2004	INTERNA AZZANI
5	Gestione Supplenze	INTERNA DELBARBA
6	Orario Lezioni	INTERNA AZZANI
7	Allievi	prog. GEMMA SCOLARI
8		
9	Gestioni Inventario	INTERNA MODIANO
10	Gestione Acquisti	prog. GEMMA SCOLARI
11	Protocollo	ARGO
12	Visualtime	TOSINI
13	wintax	TELECOM
	Registrazione	
14	assenze allievi	INTERNA DEL BARBA

MISURE DI CARATTERE ELETTRONICO/INFORMATICO

Le misure di carattere elettronico/informatico¹ adottate sono:

- utilizzo di server con configurazioni di ridondanza *attiva in doppio livello di ridondanza (doppio HD sul server più backup)*
- presenza di gruppi di continuità elettrica per il server ;
- E' attivo un firewall con hardware dedicato per proteggere la rete dagli accessi indesiderati attraverso internet ; (*Firewall- Proxy CensorNet sulla rete Didattica + singoli Firewall software sui Server principali*)
- E' attivo un sistema di definizione delle regole per la gestione delle password per i sistemi dotati di sistemi operativi Windows 2000 e XP, di seguito specificate;
- divieto di memorizzare dati personali, sensibili, giudiziari sulle postazioni di lavoro con sistemi operativi Windows 9x e Windows Me;
- E' stato installato un sistema antivirus(Norton Antivirus) su tutti le postazioni di lavoro, tale sistema è configurato per controllare la posta in ingresso, la posta in uscita, per eseguire la procedura di aggiornamento in automatico con frequenza settimanale e la scansione periodica dei supporti di memoria;
- 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;
- E' attiva la separazione della rete locale delle segreterie da quella dei laboratori didattici

REGOLE PER LA GESTIONE DELLE PASSWORD²

User-id e password iniziali sono assegnati, dal custode delle password.

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 DSGA, il quale provvede a metterla nella cassaforte in un plico sigillato.

Ogni tre mesi ciascun incaricato provvede a sostituire la propria password e a consegnare al DSGA una busta chiusa sulla quale è indicato il proprio user-id e al cui interno è contenuta la nuova password; il DSGA provvederà a sostituire la precedente busta con quest' ultima.

Le buste sono conservate nella cassaforte situata nell'ufficio del DSGA.

Le password verranno automaticamente disattivate dopo sei 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 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;*

¹ 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.

² 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.

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

- *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 CD sono conservate nella cassaforte sita nell'ufficio del DSGA*
- *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 e linee telefoniche.*

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 *denominato segreteria di presidenza* e l'utilizzo è consentito unicamente agli incaricati del trattamento (*come da tabella 3 all.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 VIRUS³

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

- *divieto di lavorare con diritti di amministratore o superutente sui sistemi operativi che supportano la multiutenza;*
- *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);*
- *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 reinstallare 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 prestare particolare attenzione al manifestarsi di nuovi malfunzionamenti nel riprendere il lavoro di routine.*

³ Le più recenti statistiche internazionali citano il virus informatico come la minaccia più ricorrente ed efficace

INCIDENT RESPONSE E RIPRISTINO⁴

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 riaccess⁵**;
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.

⁴ 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.

⁵ 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.

Tabella 3 - Procedure di spegnimento

Sistema operativo	Azione
MS DOS	<ol style="list-style-type: none">1. Fotografare lo schermo e documentare i programmi che sono attivi.2. Staccare la spina dalla presa di corrente.
UNIX/Linux	<ol style="list-style-type: none">1. Fotografare lo schermo e documentare i programmi che sono attivi.2. Se la password di root è disponibile eseguire il comando su e poi i comandi sync e halt.3. Se la password di root non è disponibile staccare la spina dalla presa di corrente.
Mac	<ol style="list-style-type: none">1. Fotografare lo schermo e documentare i programmi che sono attivi.2. Cliccare Special.3. Cliccare Shutdown.4. Una finestra indicherà che è possibile spegnere il sistema.5. Staccare la spina dalla presa di corrente.
Windows 98/NT/2000/XP	<ol style="list-style-type: none">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)

Brescia, 30.03.2009

IL TITOLARE DEL TRATTAMENTO
(Arturo Montanini)