I.P.S.S.A.R.
ISTITUTO PROFESSIONALE DI STATO PER I SERVIZI ALBERGHIERI E DELLA RISTORAZIONE
"Alfredo BELTRAME"

Via Carso, 114 - 31029 VITTORIO VENETO (TV) –- Tel.0438556128 –
E_mail: beltrame@alberghierobeltrame.gov.it – Http://www.alberghierobeltrame.gov.it

C.F. 93005790261

DOCUMENTO PROGRAMMATICO SULLA SICUREZZA
Predisposto ai sensi dell'articolo 34, comma 1, punto G) del D.Lgs. 196/2003 e del suo Allegato B "Disciplinare Tecnico in materia di misure minime di sicurezza" (art. da 33 a 36 del Codice)

Prot. n. Vittorio Veneto, 16.02.2016

PREMESSA GENERALE:

Oggi 16.02.2016 presenti il Titolare della Privacy CAVALLINI LETIZIA, il Responsabile della privacy DSGA DE MARCHI GIANNA e gli Amministratori di sistema Assistente Tecnico Sig. PALATINO GIUSEPPE e l'incaricato della custodia delle parole chiave e codici identificativi Assistente Amministrativo Sig. MODOLO FABIO, è stato revisionato il Documento Programmatico sulla sicurezza come previsto dal Decreto Legislativo 30 giugno 2003 n. 196 recante il Codice in materia di protezione di dati personali e segnatamente gli articoli 34 e seguenti, nonché l'allegato B - Disciplinare tecnico in materia di misure minime di sicurezza - dove viene specificato che:

1. Entro il 16 FEBBRAIO 2016, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:
1.1. l'elenco dei trattamenti di dati personali;
1.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
1.3. l'analisi dei rischi che incombono sui dati;
1.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
1.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;
1.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione é programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;
1.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;
1.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Per la revisione si è tenuto conto anche

- dell'introduzione del **"Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione"**, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali», pubblicato in Gazzetta Ufficiale N. 11 del 15 Gennaio 2007.
Pertanto nella verifica degli adempimenti è stato verificato che i documenti prodotti (in particolare informative e lettere di nomina) siano conformi ai dettami del regolamento stesso in particolare per quanto concerne
-Quali operazioni di trattamento sono eseguibili per ciascuna finalità
-Quali tipi di dati sensibili o giudiziari possono essere trattati per ciascuna finalità.

-dei provvedimenti relativi alle "**Linee Guida per la gestione dei lavoratori dipendenti in ambito pubblico"** e **"Linee Guida per l'uso di Internet e della Posta Elettronica";** in particolare relativamente all'utilizzo di posta elettronica e Internet da parte degli incaricati del trattamento è stato emanato un disciplinare ad integrazione delle lettere di nomina

-del provvedimento del 27 novembre 2008 **"Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema",** secondo il quale il titolare del trattamento è tenuto nell'attribuzione delle funzioni di amministratore di sistema a:
-valutare le caratteristiche soggettive di esperienza, capacità e affidabilità del soggetto designato, il quale deve fornire idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza;

-designare individualmente e con indicazione dell'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;

-redigere l'elenco degli amministratori di sistema indicando nel presente documento gli estremi identificativi delle persone fisiche amministratori di sistema, con l'elenco delle funzioni ad essi attribuite;
- rendere nota o conoscibile l'identità degli amministratori di sistema nell'ambito della propria organizzazione, mediante strumenti di comunicazione quale circolare interna qualora l'attività degli amministratori di sistema riguardi anche indirettamente servizi o sistemi che trattano o che permettono il trattamento di informazioni di carattere personale dei lavoratori;

-nel caso di servizi di amministrazione di sistema affidati in outsourcing conservare direttamente e specificamente, per ogni eventuale evenienza, gli estremi identificativi delle persone fisiche preposte a tale attività;

-verificare le attività e l'operato dell'amministratore di sistema con cadenza annuale in modo da controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza riguardanti i trattamenti dei dati personali previste dalle norme vigenti;

-registrare gli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema in modo che gli stessi comprendano i riferimenti temporali e la descrizione dell'evento che le ha generate; le registrazioni saranno conservate per almeno sei mesi.

INDICE

1. DATI GENERALI

Indicazione delle sedi:

SEDE PRINCIPALE
ISTITUTO PROFESSIONALE DI STATO PER I SERVIZI ALBERGHIERI E DELLA RISTORAZIONE "Alfredo Beltrame"
Via Carso, 114 – 31029 VITTORIO VENETO (TV)

SEDE STACCATA "DA PONTE"
Via dello Stadio, n.1 – 31029 VITTORIO VENETO (TV)

Titolare del Trattamento:
Dirigente Scolastico PRO – TEMPORE DOTT.SSA CAVALLINI LETIZIA
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.

Responsabile del Trattamento:
D.S.G.A. PRO – TEMPORE RAG. DE MARCHI GIANNA
E' 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 previo supporto dei Referenti. Il responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

Responsabili degli archivi di dati sensibili e custodi delle chiavi, designati dal D.S.G.A.:
Gli assistenti amministrativi nominati come responsabili degli archivi di dati sensibili sovrintendono gli accessi e i trattamenti effettuati sugli stessi da parte del personale autorizzato da una lettera di incarico; tali archivi sono custoditi in armadi o contenitori muniti di serratura e a questo proposito gli stessi assistenti amministrativi sono nominati custodi delle chiavi, una cui copia è presente presso l'ufficio DSGA. Nel caso di assenza o impossibilità ad effettuare le funzioni di responsabile, la responsabilità passa provvisoriamente al personale in servizio con più anzianità di servizio.

Lista responsabili esterni ed interni

ESTERNI:

- Responsabile manutenzione ed assistenza programmi Infoschool	Ditta Spaggiari di Parma (Infoschool rilevata da Spaggiari)
- Responsabile assistenza dei server e del firewall	Ditta EopenSystem di Martellago (VE)

INTERNI:

- RSPP Responsabile della Sicurezza	Ins.	Trizzino Stefano
- Rappresentante dei lavoratori per la Sicurezza	Ins.	De Simio Anna
- R.S.U. d'Istituto	Ins.	De Simio Anna
- R.S.U. d'Istituto	Ins.	Trizzino Stefano
. R.S.U. d'Istituto	ins.	Botta Serenella
- Responsabile Funzione strumentale " E-learning/Gestione sito/Formazione TIC"	Ins.	Calipari Domenico e Fornasier Angelo
- Responsabile Funzione strumentale " Tirocini/Stage"	Ins.	Anello Pignatello
- Responsabile Funzione strumentale " Alternanza Scuola Lavoro"	Ins.	Tomasi Paola
- Responsabile Funzione strumentale " Orientamento e prevenzione"	Ins.	Avon Cristina
- Responsabile Funzione strumentale " Innovazione e didattica per competenze"	Ins.	Senzani Anna
- Responsabile Funzione strumentale " Integrazione alunni con disabilità"	Ins.	Monte Mirto Renato

La lista sopra descritta è stata aggiornata con tutte le modifiche intervenute nel periodo 30.04.14 – 16.02.16 per quanto concerne i nuovi Responsabili assegnati e l'eventuale cessazione di incarichi, fermo restando che la lettera per prestatori di servizi esterni e la nomina a responsabile interno (unitamente all'informativa per i responsabili) viene attribuita immediatamente al momento dell'acquisizione dell'incarico stesso.

Amministratore di Sistema e

Assistente Tecnico di Informatica PALATINO GIUSEPPE.

Come previsto del provvedimenti del 27 novembre 2008 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" di seguito il titolare del trattamento elenca le Funzioni e i compiti dell'amministratore di sistema:

Il nominato amministratore di sistema avrà il compito di generare, sostituire ed invalidare, in relazione agli strumenti ed alle applicazioni informatiche utilizzate e secondo aggiornati criteri tecnici e di sicurezza, le parole chiave ed i codici identificativi personali da assegnare agli incaricati del trattamento dei dati personali.
Il nominato amministratore dovrà adottare programmi antivirus, firewall, ed altri strumenti sia software che hardware, che garantiscano, anche in base alle conoscenze tecniche acquisite in base al progresso tecnico, la sicurezza nel trattamento dei dati personali secondo i criteri generali stabiliti dall'art. 31 del d.lgs 196/03 e dalle previsioni contenute nell'allegato B e negli articoli 33-36 del decreto stesso.
Il nominato amministratore di sistema avrà il compito di controllare periodicamente l'efficienza dei sistemi tecnici, comunque adottati, per verificarne la validità, anche secondo consolidati criteri tecnici di valutazione.
Di detti controlli l'amministratore dovrà redigere un apposito verbale che dovrà contenere l'indicazione di coloro che vi hanno partecipato, le modalità di controllo effettuato ed altresì gli strumenti - di qualsiasi natura - utilizzati per provvedervi, i risultati ottenuti ed eventualmente gli ulteriori accorgimenti da adottare onde implementare la sicurezza del trattamento. Qualora terzi esterni intervengano sugli elaboratori vigilerà al fine di impedire il trattamento dei dati in essi contenuti
Il nominato amministratore avrà altresì il compito di vigilare - secondo le prassi istituite ed in accordo con gli altri collaboratori del titolare - che gli individuati incaricati al trattamento dei dati personali si attengano alle procedure di volta in volta indicate specificamente, sia oralmente che per iscritto, anche in ordine alla custodia e segretezza della parola chiave (e/o dei codici identificativi) loro assegnata ed altresì in relazione all'applicazione delle misure organizzative, fisiche e logiche sulla sicurezza nel trattamento.
Il nominato amministratore di sistema dovrà almeno annualmente redigere - qualora adottato - la parte del documento programmatico sulla sicurezza relativa a tutta l'attività logica di trattamento dei dati che si svolge mediante reti di elaboratori o terminali sia accessibili che non accessibili al pubblico attraverso reti di telecomunicazioni ed assistere il titolare e il responsabile del trattamento nella individuazione degli altri criteri di sicurezza da adottare sia organizzativi che fisici**.**
Il nominato amministratore dovrà anche individuare, unitamente al titolare e/o al responsabile del trattamento dei dati, le modalità e le procedure di reimpiego dei supporti di memorizzazione logica ex allegato D d.lgs 196/03 e, se del caso, individuare gli strumenti e le procedure adeguate per procedere alla distruzione e smaltimento dei supporti di memorizzazione che non possono essere riutilizzati. L' amministratore di sistema unitamente al titolare e/o responsabile del trattamento redigerà in ogni caso un apposito verbale in cui siano indicati i supporti che possono essere reimpiegati e /o distrutti, le modalità tecniche adottate sia nel caso di reimpiego che di distruzione e le persone alle quali dette incombenze siano affidate.
L'amministratore di sistema avrà cura di consegnare in ordine e in apposito registro le credenziali e password assegnate all'incaricato alla custodia delle parole chiave e codici identificativi
Si richiamata per le istruzioni e i compiti dell'amministratore la lettera di nomina assegnata ai soggetti designati.

Incaricato alla Custodia delle parole chiave e codici identificativi:
L'incaricato alla custodia delle parole chiave e dei codici identificativi assistente amministrativo MODOLO FABIO avrà cura di verificare la corretta consegna e conservare quanto consegnato in apposito registro in cassaforte in presidenza.

Incaricati al trattamento dei dati personali e comuni:

-Unità organizzativa "Collaboratori scolastici " ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A1**
-Unità organizzativa "Assistenti tecnici " ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A1**

-Unità organizzativa "Assistenti tecnici Autisti"
ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A1**

-Unità organizzativa "Personale ufficio didattica"
ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A1**

-Unità organizzativa " Personale ufficio magazzino e acquisti"
ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A1**

-Unità organizzativa "Personale ufficio personale"
ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A1**

-Unità organizzativa " Personale ufficio protocollo"
ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A1**

-Unità organizzativa " Personale ufficio contabilità"
ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A1**

-Unità organizzativa "Collaboratori del Dirigente Scolastico " Firme in calce alla lettera di incarico

-Unità organizzativa "Docenti" ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A2**

-Unità organizzativa "Membri organi collegiali interni" ELENCO NOMINATIVI CONTENUTO NELL'ALLEGATO **A3**

Ogni incaricato è stato nominato per iscritto ed ha avuto una nomina univoca e completa di istruzioni; in occasione dell'introduzione del disciplinare per l'utilizzo di Internet e della posta elettronica da parte degli incaricati del trattamento, lo stesso è stato consegnato ad ogni incaricato ad integrazione della nomina di cui sopra.
Ogni incaricato ha accesso ai soli dati relativi al suo profilo di autorizzazione.
Le liste sopra descritte sono state aggiornate con tutte le modifiche intervenute nel periodo 31.03.12 – 16.02.2016 per quanto concerne i nuovi incaricati assegnati e l'eventuale cessazione di incarichi, fermo restando che la lettera di nomina come incaricato del trattamento (unitamente all'informativa per il personale dipendente) viene attribuita immediatamente al momento dell'acquisizione dell'incarico stesso.

2. MISURE FISICHE

Il trattamento di tutti i dati viene effettuato presso i seguenti locali:

LOCALE	TIPO DI ACCESSO	SERRATURA	SISTEMA DI ACCESSO
UFFICIO DSGA	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
SEGRETERIA AMMINISTRATIVA/CONTABILITA'	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
PROTOCOLLO	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
SEGRETERIA DEL PERSONALE	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
SEGRETERIA DIDATTICA	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
UFFICIO TECNICO / MAGAZZINO	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
UFFICIO COLLABORATORI D.S .	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
UFFICIO DIRIGENTE SCOLASTICO	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
UFFICIO COLLABORATORI D.S.	Solo autorizzati Con orario di ricevimento	SI	Porta con chiave
PORTINERIA	Libero in presenza del personale	SI	Porta con chiave
AULA INSEGNANTI	Libero in presenza del personale	SI	Porta con chiave
AULE DIDATTICHE	Libero in presenza del personale	SI	Porta con chiave

3. COMPUTER E SISTEMI PRESENTI NELL'ISTITUTO

Elenco dei computer presenti nella sede:

N	CODIFICA		DESCRIZIONE PC	SISTEMA OPERATIVO	SUPPORTI REMOVIBILI	ANTIVIRUS/ANTISPYWARE	FIREWALL
1	Ads	dirigente scol.	PERSONAL COMPUTER PCL-CON12L2P6001 LENOVO THINKCENTRE M93	WINDOWS 8 PROFESSIONAL	cd-dvd - penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
2	Ads01	dirigente scol.	Notebook Asus PU551 DS - Pro - Processore Intel Core i7 (4 gen) 4510U – 3,1 GHz - Memory 16 GB DDR3 Memoria 1 TB HDD / 7200 rpm + SSD 850 EVO 500GB	Windows 7 Professional precaricato E licenza Windows 8.1	cd-dvd - penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
3	Adsga	DSGA	Pc Hyunday - Intel Celeron CPU - 4,00 Gb RAM - S.O. 64 bit	Win 7 Pro service pack1	cd-dvd penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
4	Acont02	contabilità 1	Pc Hyunday - Intel Celeron CPU - 4,00 Gb RAM - S.O. 64 bit	Win 7 Pro service pack1	cd-dvd penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240

5	Acont03	contabilità 2	FUJITSU Pentium Dual Core CPU E5400	Windows 7 Professional	cd-dvd penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
6	Adid0l	Didattica 1	PERSONAL COMPUTER PCL-CON12L2P6001 LENOVO THINKCENTRE M93	WINDOWS 8 PROFESSIONAL	cd-dvd - penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
7	Aprot0l	protocollo	Pc Hyunday - Intel Celeron CPU - 4,00 Gb RAM - S.O. 64 bit	Win 7 Pro service pack1	cd-dvd penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
8	Apers01	personale 1	Pc Hyunday - Intel Celeron CPU - 4,00 Gb RAM - S.O. 64 bit	Win 7 Pro service pack1	cd-dvd penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
9	Apers03	personale 3	PERSONAL COMPUTER PCL-CON12L2P6001 LENOVO THINKCENTRE M93	WINDOWS 8 PROFESSIONAL	cd-dvd - penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
10	Apers04	personale 4	PERSONAL COMPUTER PCL-CON12L2P6001 LENOVO THINKCENTRE M93	WINDOWS 8 PROFESSIONAL	cd-dvd - penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
11	Apcassenze	Uff. Vicario	C.D.C. AMD Athlon XP 1800 334MB RAM client	Win XP Pro service pack3	cd-dvd floppy-penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
12	Balim	magazz. aliment.	PERSONAL COMPUTER PCL-CON12L2P6001 LENOVO THINKCENTRE M93	WINDOWS 8 PROFESSIONAL	cd-dvd - penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
13	Bmag01	magazz. amm.	PERSONAL COMPUTER PCL-CON12L2P6001 LENOVO THINKCENTRE M93	WINDOWS 8 PROFESSIONAL	cd-dvd - penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
14	Bimag02	magazz. ainm. 1	Pc Hyunday - Intel Celeron CPU - 4,00 Gb RAM - S.O. 64 bit	**Win 7 Pro service pack1**	cd-dvd -penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
15	Bmag()3	magazz. amm. 2	Pc Hyunday - Intel Celeron CPU - 4,00 Gb RAM - S.O. 64 bit	**Win 7 Pro service pack1**	cd-dvd -penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
16	Bmag()4	magazz. amm. 3	PERSONAL COMPUTER PCL-CON12L2P6001 LENOVO THINKCENTRE M93	WINDOWS 8 PROFESSIONAL	cd-dvd - penna usb	ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240
17	Srv2k3l1	server segreteria	DELL Power Edge t 420	Win Server 2008.	cd-dvd-tape	AVG Server 2013 Business Edition (Grisoft) ANTIVIRUS G DATA CLIENT SECURITY BUSINESS PC 2014 ILLIMITATI 36 MESI	SonicWall 240

4. CENSIMENTO ARCHIVI INFORMATICI (elenco trattamenti e distribuzioni responsabilità)

Elenco degli Archivi presenti nelle sedi dettagliati nell' allegato **A01**

5. MISURE LOGICHE

1. Ogni incaricato è dotato di password e username univoci e personali costituenti le sue credenziali di autenticazione.
2. Le password sono cambiate almeno ogni tre mesi (per i dati particolari) con le procedure di cui alla legge. Per i dati personali sono cambiate almeno ogni sei mesi.
3. I codici identificativi personali sono disattivati in caso di non utilizzo per più di sei mesi.
4. Ai dati particolari hanno accesso solo ed esclusivamente gli incaricati grazie ad un sistema di verifica che gli permette di accedere ad un server riservato - oppure – alla parte dell'elaboratore in cui sono conservati i dati particolari.
5. Gli antivirus sono aggiornati con le nuove impronte virali ogni giorno.

6. Periodicamente viene chiesta la verifica dell'efficienza del firewall alla Ditta "Eopensystem", che provvede anche agli aggiornamenti.
7. I sistemi sono stati studiati in maniera da autoprevenire le intrusioni. Tutti i sistemi sono periodicamente verificati dagli amministratori di sistema.
8. L'azienda adotta le procedure di esecuzione back up riportate al punto **7** del presente DPS.
9. I supporti di memorizzazione removibili contenenti dati particolari se non utilizzati sono distrutti o resi inutilizzati attraverso appositi sistemi di distruzione. Qualora non siano recuperabili i dati, i supporti possono essere riutilizzati.

6. CRITERI E MODALITA' DI RIPRISTINO DELLA DISPONIBILITA' DEI DATI

CONSEGUENZE IPOTIZZABILI IN CASO DI PERDITA DI DATI:

PREMESSA: I dati trattati dalla scuola in forma elettronica sono generalmente contenuti anche nei documenti cartacei dalla stessa gestiti (originali) in quanto servono:
-per produrre documenti cartacei che sono conservati e che sono gli unici documenti ad avere valore legale;
-per elaborare dati provenienti da documenti cartacei che sono conservati e che sono gli unici documenti ad avere valore legale;
-per produrre comunicazioni ad altri Enti (Tesoro, Ministero della Funzione Pubblica, MIUR, ecc.) e cessa la necessità di conservarli in forma elettronica non appena la comunicazione ha avuto effetto;
-per ricevere comunicazioni provenienti dall'esterno, delle quali di norma si fa immediatamente la copia cartacea, che viene poi conservata e che è l'unica ad avere valore legale.
-per produrre determinati allegati che non si ritiene utile stampare e determinati programmi che non è, ovviamente, possibile stampare. In entrambi i casi non si tratta mai di dati personali, né di software che tratti dati personali.
Inoltre possiamo definire basso il grado di urgenza con cui all'Interessato possono servire i documenti necessariamente prodotti tramite computer.
Poiché esiste un periodico back-up, le analisi che seguono riguardano la perdita di dati non ancora salvati (quindi una settimana al massimo, circa).

Ci sono programmi elettronici che contengono dati la cui perdita è pregiudicante (massimo una settimana perché il back up avviene almeno una volta alla settimana)
Il programma gestione finanziaria, che consente di emettere mandati e riversali è sicuramente quello che potrebbe soffrire non tanto della perdita dei dati quanto del breve blocco operativo conseguente alla necessità di reinserire i dati perduti, dei quali comunque esistono i documenti cartacei facilmente rintracciabili.
Anche il programma stipendi, il programma assenze e il programma alunni creerebbero notevoli perdite di tempo per reintegrare i dati, tuttavia la perdita non sarebbe irreversibile né di per sé grave.

Conseguenze di un blocco di computer di breve durata (1 giorno circa)
Nel caso di blocco :
- di un solo computer isolato (=non in rete) che fosse l'unico ad aver memorizzati certi dati e certi programmi,
- del server di rete in cui siano memorizzati tutti i dati e i programmi
si ritiene che il danno sarebbe minimo perché rarissimamente la scuola opera con scadenze in tempo reale, quindi l'attesa di un giorno non creerebbe problemi a meno che non si fosse atteso l'ultimissimo momento per un adempimento con scadenza tassativa.
Nel caso che tale guasto riguardasse un terminale di rete (client), se i dati e i programmi di lavorazione dei dati sono memorizzati nel server, passando a un altro terminale si risolve il problema senza inconvenienti.

Blocco del computer principale (o unico) collegato a Internet
Per quanto riguarda le comunicazioni di posta elettronica o fatte tramite internet, utilizzando il computer come terminale remoto, va precisato che raramente ci sono messaggi di posta elettronica che non possano attendere un giorno o comunicazioni che non possano ugualmente essere procrastinate. Va tuttavia riconosciuto che sarebbe buona norma avere, comunque, almeno due computers in grado di compiere tali operazioni. Ciò significa che il computer "di riserva":
deve essere collegabile a internet di fatto o potenzialmente in pochi minuti. Deve avere già caricati eventuali programmi che sono necessari per emulare un terminale remoto o per comunicare con determinati enti .

Conseguenze di un blocco di computer di media-lunga durata (oltre 1 giorno)
Nel caso di blocco prolungato:
a) di un solo computer isolato (=non in rete) che fosse l'unico ad aver memorizzati certi dati e certi programmi,
b) del server di rete in cui siano memorizzati tutti i dati e i programmi
c) dell'intero sistema
si ritiene che il danno diventerebbe serio, grave dopo circa 3-4 giorni, gravissimo dopo una settimana.
Invece, nel caso che tale guasto riguardasse un terminale di rete (client), se i dati e i programmi di lavorazione dei dati sono memorizzati nel server, passando a un altro terminale si risolve il problema senza inconvenienti.
Per intervenire nei casi a), b), c) è normalmente sufficiente una procedura di "Disaster Recovery" (= Recupero di un disastro, che ha provocato la messa fuori uso completa e prolungata, a volte irreversibile, del sistema informatico o di sue parti vitali a causa di un evento). Se essa si conclude in uno, massimo due giorni, è accettabile, mentre non sembra indispensabile un piano di continuità operativa che riduca necessariamente i tempi di sosta sotto uno-due giorni. I costi economici sarebbero infinitamente superiori ai costi dovuti al blocco temporaneo.

Procedure di "Disaster Recovery"
Nell'ipotesi che un evento distrugga o renda indisponibili tutti i computers, l'Istituto
1) tramite l'amministratore di sistema nominato e i tecnici informatici di supporto verifica il reale stato della situazione;
2) una volta verificato l'impossibilità di agire personalmente sulla situazione si rivolge alla ditta di assistenza hardware e/o software esterna cui ha affidato l'incarico di manutenzione del sistema informatico stesso in caso di eventi non gestibili internamente.

Piano di continuità
I programmi originali di tutto il software necessario sono collocati nell'armadio di sicurezza di cui si è accennato, in modo che siano sempre disponibili e che l'evento disastroso abbia minime possibilità di distruggerli.

Prove di ripristino dei dati
Per evitare errori umani, procedurali, organizzativi o delle macchine, verranno periodicamente eseguiti test di ripristino (ovviamente dopo aver salvato i dati correnti oppure, preferibilmente, su un computer diverso da quello dove sono i dati correnti).
Per non avere problemi, anche in vista dell'implementazione di misure di disaster recovery e di un piano di continuità, il test verrà eseguito su un computer diverso da quelli dove risiedono gli archivi elettronici da ripristinare. Nell'occasione si farà quindi anche una prova di disaster recovery, caricando prima i programmi che servono per gestire i dati e successivamente facendo il test di ripristino.
Alla fine della prova i dati verranno cancellati, ma non i programmi (sempre che le licenze d'uso lo consentano) in modo che quel computer sia già predisposto per il disaster recovery.

Alle prove sarà presente un tecnico informatico per dare utili consigli e sovrintendere all'esecuzione. Saranno presenti tutti gli Incaricati che hanno avuto l'istruzione di realizzare il back-up periodico di un archivio elettronico, allo scopo anche che comprendano meglio a cosa serve e siano più motivati psicologicamente.

7. PROCEDURE E MODALITÀ' DI BACK UP

I sistema informatico dell'IPSSAR"Alfredo Beltrame" è ovviamente caratterizzato dalla presenza al suo interno di dati, applicazioni e altro; la natura di queste informazioni è variabile in relazione alla funzione che in concreto il sistema svolge ma, in ogni caso, la loro importanza evidenzia la necessità di predisporre delle misure idonee ad impedire la loro distruzione e/o danneggiamento e, comunque, a rendere possibile il loro ripristino in tempi brevi senza che questo comporti delle conseguenze negative sotto il profilo economico, legale, o puramente di immagine.
A tal fine l'esecuzione periodica e programmata di procedure di backup consente di far fronte agevolmente a tutte quelle situazioni in cui sussiste una esigenza di immediato recupero dei dati a prescindere dalla causa della loro alterazione e/o perdita come virus, guasti hardware, attacchi informatici, ecc....
Tutti i PC della segreteria, dislocati nei vari uffici posti all'entrata dell'Istituto su ambo i lati (2 in ufficio didattica/protocollo, 1 in archivio didattico, 2 in ufficio personale, 2 in ufficio contabilità, 3 in ufficio magazzino, 1 in magazzino alimentari, 1 in ufficio del DSGA, 1 in ufficio vicepresidenza e 1 in ufficio del Dirigente Scolastico) fanno parte di una rete lan (dominio segreteria).
Gli altri PC (laboratori, aula docenti, ufficio Vicario, ufficio funzioni strumentali, aula diversamente abili, aula polifunzionale e uffici tecnici informatica e tecnici della ristorazione) che si trovano nell'edificio scolastico fanno parte di un altra lan (dominio laboratori).
Gli altri PC (laboratori, aula docenti, ufficio Vicario, ufficio funzioni strumentali, aula diversamente abili, aula polifunzionale e uffici tecnici informatica) che si trovano nell'edificio scolastico fanno parte di un altra lan (dominio laboratori).
La gestione delle 2 reti, cablate con cavi cat. 6, è affidata a 2 server Dell che si trovano nella stanza n. 21 situata al piano terra ala ovest, alla quale hanno accesso le persone (amministratori di rete) incaricate dal DS.
La sicurezza dei dati è affidata ad un firewall hardware "Sonicwall 240" che oltre a proteggere da attacchi esterni, tramite un programma interno (CONTENT FILTERING) permette o nega la connessione in uscita e le relative richieste secondo quanto stabilito da una policy scolastica in relazione all'utilizzo di Internet a seconda delle esigenze.
Oltre al firewall ogni pc è dotato dell'antivirus "GDATA SECURITY BUSINESS" che include un antispyware, una funzione di scansione dei link utile durante la navigazione sul web (compatibile con Internet Explorer e Firefox), la possibilità di analizzare le e-mail in entrata e in uscita e stare al sicuro da allegati infetti e persino un antirootkit e uno strumento di protezione dal furto di identità.che vengono aggiornati in modo automatico.
Nel server della segreteria, i dati, gli applicativi, i gestionali, entratel, posta elettronica e quant'altro vengono gestiti in modo ridondato con tecnologia RAID 5 .
A tale scopo il server, per essere sicuri di non perdere i dati salvati nel supporto rigido per cause descritte sopra, è dotato di un sistema di backup, salvataggio dati su disco di rete (NAS) mediante un software (Veritas Symantec Backup) permette il salvataggio giornaliero di tutto il traffico informatico che avviene nella rete della segreteria. Il salvataggio dati su disco di rete è ubicato in locale diverso da quello server.
I pc server inoltre sono assistiti da un U.P.S. (gruppo di continuità), il quale supplisce per un certo periodo alla mancanza di alimentazione elettrica.
Sono accreditati al dominio "laboratori" tutti i docenti, gli studenti, il personale ata e gli esperti esterni.
E' accreditato al dominio "segreteria" tutto il personale di segreteria, il Dirigente Scolastico e la Vicepreside.
In tal modo il dominio, gestito attraverso la piattaforma Active directory, del S.O. Windows 2008 Server che è un insieme integrato di servizi, contribuisce a migliorare le funzionalità di gestione, protezione e quindi la gestione della privacy del sistema operativo di rete.
I due domini sono distinti e non c'è alcuna relazione o collegamento tra di essi.

8. ELENCO TRATTAMENTI E DISTRIBUZIONE RESPONSABILITA'

Elenco trattamenti e distribuzione responsabilità dettagliate nell'allegato **A01.**

9. PREVISIONI E ANALISI DEI RISCHI

1		2		3
Evento		Impatto sulla sicurezza dei dati		Rif .misure d'azione
		Descrizione	Gravità stimata	
Comportamenti degli operatori	Furto delle credenziali di autenticazione	Accesso non autorizzato al computer	bassa	Istruzioni agli Incaricati, formazione, azione del "Custode delle Parole-chiave", controllo dell'accesso ai locali che sono chiusi a chiave quando non presidiati, divieto di accesso ai locali alle persone non autrorizzate

	carenza di consapevolezza, disattenzione o incuria	Le credenziali perdono riservatezza o dati sono inutilmente resi visibili	bassa	Come precedente
	comportamenti sleali o fraudolenti	Accesso per fini personali ai dati (che però sono poco appetibili), che vengono conosciuti da Incaricati che non ne hanno diritto	bassa	Come precedente, inoltre: eventuale creazione di profili di autorizzazione diversificati e utilizzo cifratura per i rari files contenenti dati sensibili, giudiziari o particolari importanti.
	errore materiale	Cancellazione o perdita di dati	Bassa (esiste copia cartacea di tutto)	Formazione degli incaricati, profilo di autorizzazione che non consenta la formattazione dei dischi fissi o la cancellazione di files importanti.
Eventi relativi agli strumenti	azione di *virus* informatici o di codici malefici	Cancellazione di dati, malfunzionamenti o blocco del sistema, trasmissione casuale di dati a indirizzi di posta elettronica memorizzati, confusione con incapacità di individuare dati utili	elevata	Regolare aggiornamento dell'antivirus e del sistema operativo, con istruzioni agli incaricati e monitoraggio di controllo sull'effettiva attuazione,
	spamming (posta indesiderata e disturbante) o altre tecniche di sabotaggio	Confusione con rischio di non individuazione di messaggi utili o di loro cancellazione per errore	Medio/alta	filtro antispamming, formazione degli Incaricati a riconoscere i messaggi di disturbo e a gestire le regole di assegnazione dei messaggi di posta elettronica alle varie cartelle
	mal funzionamento, indisponibilità o degrado degli strumenti	Malfunzionamenti o blocco del sistema	media	Manutenzione programmata, formazione ad individuare i sintomi di malfunzionamento per un rapido intervento, piano di backup - Distaster Recovery e di continuità operativa
	accessi esterni telematici non autorizzati	Visione indebita di dati o sabotaggio	Bassa (i dati non sono appetibili e il loro valore si basa sull'originale cartaceo)	Installazione di Firewall, con regolare aggiornamento

10. TRATTAMENTI AFFIDATI ALL'ESTERNO DELLA STRUTTURA DEL TITOLARE

Per garantire l'adozione delle misure minime di sicurezza in caso di trattamento dei dati affidati all'esterno della struttura del titolare viene inviata ai soggetti esterni (persone fisiche o giuridiche) una richiesta scritta di fornire:
-un estratto del DPS che attesti l'avvenuto adeguamento alle misure minime di sicurezza del trattamento dei dati;
-in alternativa una dichiarazione che attesti l'avvenuto adeguamento alle misure minime di sicurezza del trattamento dei dati.

11. FORMAZIONE DEGLI INCARICATI

In ottemperanza all'obbligo previsto dal D.lgs. 196/2003 di effettuare degli interventi di formazione per gli incaricati e responsabili del trattamento, ogni incaricato e/o responsabile ha ricevuto un manuale esplicativo della norma e una lettera di incarico completa di istruzioni. Inoltre in occasione della revisione del documento programmatico sulla sicurezza il personale ha ricevuto
-in data 31.03.2007 una integrazione del manuale con riferimento al "Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»
-in data 31.03.2008 una integrazione del manuale relativa agli interventi normativi intervenuti nel periodo marzo 2007 - marzo 2008.
-in data 31.03.2009 una integrazione del manuale relativa agli interventi normativi intervenuti nel periodo marzo 2008 - marzo 2009.

Sono stati, inoltre, organizzati, nel corrente anno scolastico, i sotto dettagliati corsi di formazione per il personale docente e ATA:
-corso di formazione sull'utilizzo del sistema di segreteria digitale della ditta Spaggiari al quale ha partecipato tutta la segreteria, il DSGA, il DS e i suoi collaboratori.

12. CONCLUSIONI

Il presente documento è stato aggiornato al 16.02.2016.
Le nomine sono state riviste e/o rinnovate.
Gli allegati al presente documento devono ritenersi parte integrante del documento stesso.
Per quanto riguarda il LOG degli Amministratori di Sistema si procederà all'acquisto di adeguati software ed eventuali PC.
Il DPS sarà pubblicato sul sito dell'Istituto.

ALLEGATI:

-Planimetria delle sedi
-A1 - Unità organizzativa personale ATA: Assistenti amministrativi, Assistenti Tecnici e Collaboratori scolastici
-A2 - Unità organizzativa "Docenti"
-A3 - Unità organizzativa "Membri organi collegiali interni"
-A01 - Elenco trattamenti e distribuzione responsabilità

Il Dirigente Scolastico
(Dott.ssa Cavallini Letizia)
_____