Interscreen sas di Marco Maestrini e C. – Viale Martesana 115- 20090 Vimodrone Milano (Mi).

C.C.I.A. di Milano 1303346 - Trib. Milano 290998/7400/48 - Cod. Fisc. P.IVA 09602220155
Tel: 0226809377 Fax: 0226110796 - E-mail: info@interscreen.it - Web: www.interscreen.it

CERTIFICAZIONE DELLA SUSSISTENZA DELLE MISURE MINIME DI SICUREZZA PREVISTE AGLI ARTT. 33 ss. D.Lgs 196/2003 ALL'INTERNO DI UNA INFRASTRUTTURA INFORMATICA DEPUTATA AL TRATTAMENTO DIGITALE DI DATI PERSONALI

lo scrivente

Interscreen sas di Marco Maestrini e C.

in qualità di amministratore di rete di:

Istituto Comprensivo Statale Via Maffucci
Via Maffucci, 60 20158 Milano
Codice Fiscale:97667360156 Codice Meccanografico:MIC8FP00T

- Vista l'esistenza, tra l'azienda scrivente ed il Titolare del trattamento di seguito meglio identificato, di un rapporto contrattuale di assistenza tecnica informatica.

- Letto il contenuto del Punto 25 del Capitolato tecnico (Allegato B al D.Lgs. 196/2003) recante :"*Il Titolare che adotta le misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente capitolato tecnico*"

rilascia la presente certificazione, che costituirà allegato al **Documento Programmatico sulla Sicurezza del Titolare**, per le finalità previste dalla legge.

DATA di ESECUZIONE del SOPRALLUOGO/INTERVENTO:

28/03/2017

PERSONALE INCARICATO:

Tecnico
Fabio Cavallo

DATI IDENTIFICATIVI DEL TITOLARE DEL TRATTAMENTO:

Dirigente Scolastico
Dott.ssa Laura Barbirato

DESCRIZIONE DELL'INFRASTRUTTURA INFORMATICA:

Rete informatica Client-Server sotto dominio composta da 1 server WINDOWS 2008 e da n° 10 pc client WINDOWS collegati tramite uno switch a 16 porte. Collegamento ad internet tramite firewall/router adsl.

In considerazione del fatto che, mediante l'impiego delle apparecchiature informatiche costituenti l'infrastruttura descritta in copertina, si effettua trattamento di dati personali e/ sensibili, si procede alla verifica puntuale delle seguenti modalità tecniche :

PARTE A: SISTEMA DI AUTENTICAZIONE INFORMATICA:

REQUISITO	Punto Corrispondente Allegato B	Soluzione Tecnica Adottata	
REQUISITO 1	*Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.*	Tutti gli incaricati del trattamento dei dati sono dotati di credenziali di autenticazione che consentano il superamento di una procedura di identificazione?	SI X NO
REQUISITO 2	*Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.*	Quale sistema di autenticazione è adottato?	UserID/PASSWORD X DISPOSITIVO IDENTIFICATIVO CARATTERISTICA BIOMETRICA
		Breve Descrizione: **Active directory su windows 2008 server R2**	
REQUISITO 3	*Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.*	Ad ogni incaricato è assegnata individualmente una o più credenziali di autenticazione?	SI X NO
REQUISITO 4	*Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.*	Omissis	Omissis
REQUISITO 5	*La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.*		POLICIES GLOBALI DI DOMINIO X POLICIES CONFIGURATE LOCALMENTE LA RETE INFORMATICA NON PREVEDE POLICIES
		Periodo di validità della parola chiave	3 MESI X 6 MESI
REQUISITO 6	*Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.*	Il Codice di identificazione è personale e non assegnato ad altri incaricati, neanche in tempi diversi ?	SI X NO

REQUISITO 7	*Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.*	Le credenziali non tecniche sono disattivate se non utilizzate da oltre 6 (sei) mesi?	[X] NO
		Credenziali tecniche esentate dall'obbligo di disattivazione	[X] Amministrator [X] Amministratori di Rete Amministratori di Sistema Altro
		Breve descrizione:	
REQUISITO 8	*Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.*	Le credenziali sono disattivate al venire meno della necessità di accedere ai dati personali?	[X] NO
REQUISITO 9	*Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.*	Sono impartite al personale istruzioni per non lasciare incustodita la stazione di lavoro durante le sessioni in corso ?	[X] NO
		E' impostato un salvaschermo ad attivazione automatica?	[X] SI NO
REQUISITO 10	*Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.*		Omissis
REQUISITO 11	*Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.*	I dati personali oggetto del trattamento sono soggetti alla diffusione e pertanto questa destinazione consente al titolare la non osservanza dei requisiti da 1 a 10?	SI [X] NO

PARTE B: SISTEMA DI AUTORIZZAZIONE:

REQUISITO	Punto Corrispondente Allegato B	Soluzione Tecnica Adottata	
REQUISITO 12	*Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.*	Per gli incaricati del trattamento è prevista la sussistenza di profili di autorizzazioni di ambito diverso e pertanto è implementato un sistema di autorizzazione?	X SI NO
		Breve descrizione: **profilo utente** **account AXIOSin rete**	
REQUISITO 13	*I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.*	I profili di autorizzazione di ambito diverso sono individuati e configurati preventivamente rispetto all'inizio del trattamento?	X SI NO
REQUISITO 14	*Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.*	Le condizioni che consentono di conservare ciascun profilo di autorizzazione sono verificate almeno annualmente?	X SI NO

PARTE C: ALTRE MISURE DI SICUREZZA:

REQUISITO	Punto Corrispondente Allegato B	Soluzione Tecnica Adottata
REQUISITO 15	*Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*	Al momento della redazione del presente certificato, viene redatta la lista degli incaricati del trattamento e dei relativi profili di autorizzazione (ALLEGATO 1) nonché, (solo per le istituzioni scolastiche statali) il profilo di autorizzazioni del software gestionale adottato (SISSI IN RETE, Axios, Infoschool, Proser) (ALLEGATO 2).
REQUISITO 16	*I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.*	Sono attivati strumenti idonei alla protezione dei dati personali dal rischio intrusione? **[X] SI** **[ ] NO** Breve descrizione: **Firewall Hardware Zwall5 Zyxell** Sono attivati strumenti idonei alla protezione dei dati personali dall'azione di programmi di cui all'Art. 615 quinquies del Codice Penale? **[X] SI** **[ ] NO** Breve descrizione: **Kasperski Antivirus su server Kasperski antivirus su client**
REQUISITO 17	*Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.*	Tutti i sistemi operativi client e server sono supportati dai rispettivi produttori e godono degli aggiornamenti di protezione **[X] SI** **[ ] NO** Breve descrizione: **Windows server 2008 R2 Windows 7** Si è provveduto all'installazione di aggiornamenti (patch) dei software e dei sistemi operativi con frequenza almeno annuale se il trattamento riguarda solamente dati personali o almeno semestrale se riguarda dati sensibili? **[X] SI** **[ ] NO** Frequenza degli aggiornamenti: **[X] 6 MESI** **[ ] 1 ANNO**

REQUISITO 18	*Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.*	E' previsto un sistema di salvataggio dei dati con cadenza almeno settimanale?	X NO
		Dispositivo:	Unità CD-DVD R/RW Unità Nastro Unità di memoria di massa X Server di backup
		Breve descrizione: **DISCO DI SALVATAGGIO ESTERNO SU RETE**	
		E' previsto che i supporti removibili di backup siano custoditi con cura in un luogo diverso da quello in cui è custodito il SERVER?	X NO
REQUISITO 19	*Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza*	E' stato redatto in tempo utile il Documento Programmatico sulla Sicurezza?	X NO

PARTE D: ULTERIORI MISURE IN CASO DI TRATTAMENTO DI DATI SENSIBILI O GIUDIZIARI:

REQUISITO	Punto Corrispondente Allegato B	Soluzione Tecnica Adottata	
REQUISITO 20	*I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.*	L'accesso abusivo di cui all'Art. 615 ter del Codice Penale a dati sensibili e giudiziari è impedito mediante utilizzo di idonei strumenti elettronici?	SI X NO
REQUISITO 21	*Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.*	I supporti removibili (nastri, dischetti etc.) contenenti dati sensibili o giudiziari sono gestiti e custoditi in modo da evitare accessi non autorizzati e trattamenti non consentiti?	SI X NO
REQUISITO 22	*I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.*	I supporti removibili (nastri, dischetti etc.) contenenti dati sensibili o giudiziari non più in uso sono distrutti o riutilizzati solamente dopo l'eliminazione irreversibile delle informazioni registrate?	SI X NO
REQUISITO 23	*Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.*	Esiste un processo per garantire il ripristino dell'accesso ai dati in linea entro un termine massimo di 7 (sette) giorni?	SI X NO
REQUISITO 24	*Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.*	Il Titolare del trattamento è un organismo sanitario o un soggetto esercente la professione sanitaria che tratta dati idonei a rivelare lo stato di salute e la vita sessuale delle persone?	SI NO X
		I dati sensibili suddetti, contenuti in archivi elettronici, sono trattati con tecniche di cifratura o mediante uso di codici identificativi che li rendano temporaneamente inintelleggibili?	SI X NO
		Se SI indicare il sistema impiegato:	TECNICA DI X CIFRATURA CODICI IDENTIFICATIVI
		Breve descrizione: **Software di backup Cobian Backup**	

		Il trasferimento in formato elettronico di detti dati avviene applicando sistemi di cifratura ?	SI X NO
		Breve descrizione:	

PARTE E: MISURE DI TUTELA E GARANZIA:

REQUISITO	Punto Corrispondente Allegato B	Soluzione Tecnica Adottata	
REQUISITO 25	*Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.*	E' rilasciata l'attestazione scritta di conformità degli interventi tecnici sui sistemi informativi eseguiti dai responsabili della manutenzione?	SI [X] NO [ ]
REQUISITO 26	*Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.*	Il Titolare riferisce dell'avvenuta redazione del D.P.S. nella relazione accompagnatoria del bilancio d'esercizio (se dovuta)?	SI [X] NO [ ]

PARTE F: TRATTAMENTI SENZA L'AUSILIO DI STRUMENTI ELETTRONICI:

REQUISITO	Punto Corrispondente Allegato B	Soluzione Tecnica Adottata	
REQUISITO 27	*Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l'intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.*	Le istruzioni agli incaricati sulle modalità di trattamento dei dati, anche e soprattutto per quelli cartacei, sono impartite per iscritto?	SI X NO
		Le lettere di nomina a "Incaricato del trattamento" sono confermate annualmente?	SI X NO
		E' stata nominata la figura di Amministratore di Sistema?	SI – figura interna SI – figura esterna X NO
REQUISITO 28	*Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.*	La conservazione di documenti cartacei contenenti dati sensibili o giudiziari avviene impedendo l'accesso alle persone prive di autorizzazione?	SI X NO
REQUISITO 29	*L'accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l'orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.*	L'accesso agli archivi dopo l'orario di chiusura prevede l'identificazione e la registrazione di chi vi accede?	SI X NO

DICHIARAZIONE DI CONFORMITA'

In seguito all'analisi eseguita è emerso che l'infrastruttura informatica ove avviene il trattamento dei dati personali oggetto del presente accertamento

E' CONFORME X

NON E' CONFORME

alle prescrizioni di cui agli Artt. 33 ss. del D.Lgs. 196/2003 (Codice della Privacy).

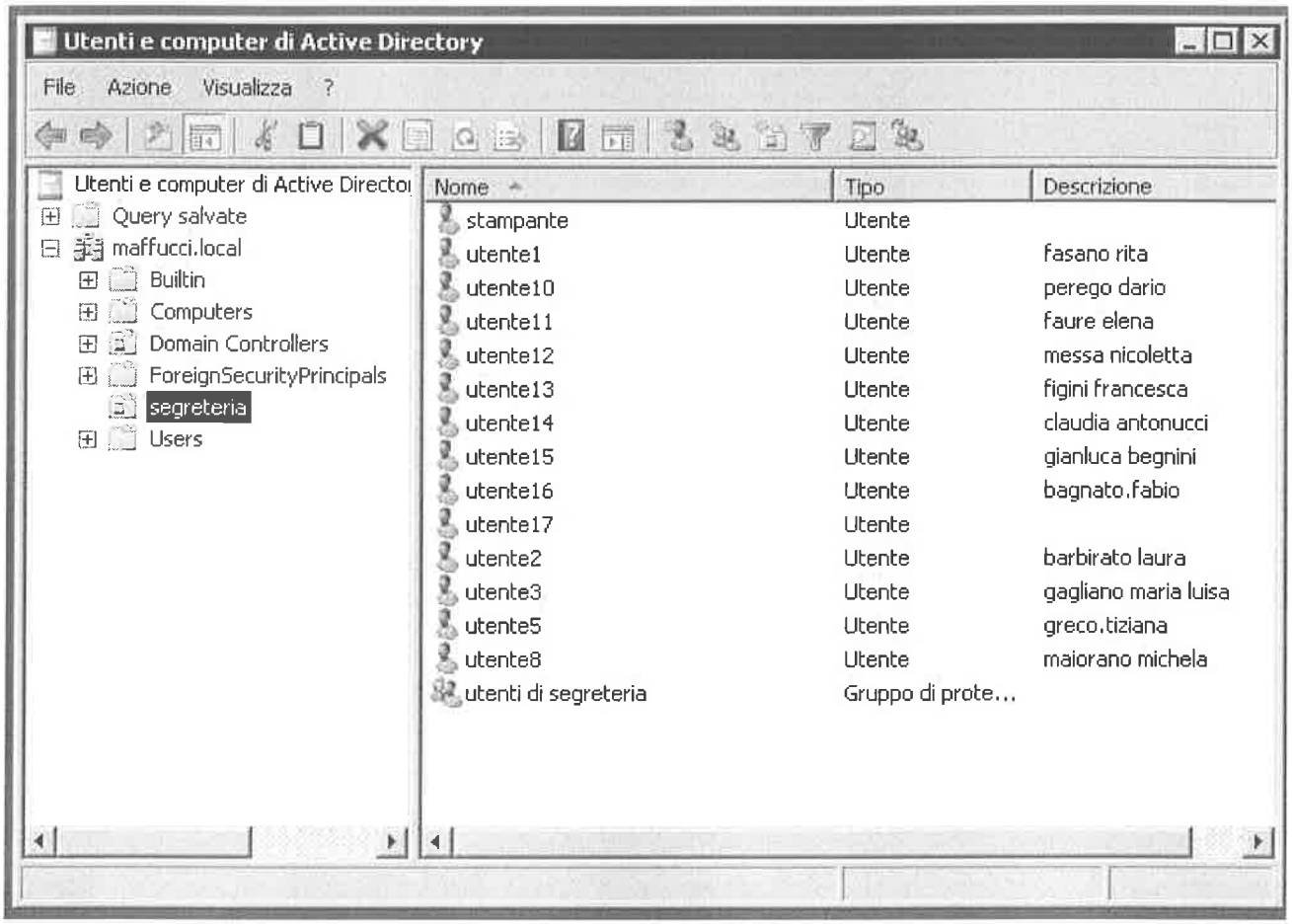
data 28/03/2017

Fabio Cavallo

FIRMA DEL FUNZIONARIO TECNICO INTERVENUTO

ALLEGATO 1

ELENCO DEI PERMESSI DI ACCESSO ALLA RETE PUBBLICA VALIDI



ALLEGATO 2 (Solo per Istituzioni Scolastiche)

Aree Abilitate	Utenti Abilitati									
	Fasano Rita	Gianluca Benigni	Faure Elena	Messa Nicoletta	Figini Francesca	Antonucci Claudia	Gagliano Maria Luisa	Tiziana Greco	Bagnato Fabio	Maiorano Michela
 Area Libri di Testo.lnk										X
 Area Magazzino.lnk	X	X								
 Area Minute Spese.lnk	X									
 Area Nuovo Bilancio.lnk	X	X								
 Area Personale.lnk	X	X				X	X	X	X	
 Area Retribuzioni.lnk	X	X				X	X		X	
 Area Alunni.lnk	X		X	X	X			X	X	X
Area Backup & Restore		X							X	
Gestione Sicurezza		X							X	
Open SISSI		X							X	
Protocollo	X	X	X			X	X	X	X	X

Interscreen sas di Marco Maestrini e C. – Viale Martesana 115- 20090 Vimodrone Milano (Mi).

C.C.I.A. di Milano 1303346 - Trib. Milano 290998/7400/48 - Cod. Fisc. P.IVA 09602220155
Tel: 0226809377 Fax: 02-26110796 - E-mail: info@interscreen.it - Web: www.interscreen.it

Milano 28/03/17

Alla cortese att.ne

DIRIGENTE : dott.ssa Laura Barbirato
DSGA: dott.ssa Rita Fasano

OGGETTO: RELAZIONE ANNUALE AMMINISTRATORE DI SISTEMA

Lo scrivente **Fabio Cavallo** nominato amministratore di sistema del vostro **Istituto Comprensivo Statale Via Maffucci Via Maffucci, 60 20158 Milano** per l'anno 2016/2017 durante l'uscita di verifica del 28/03/2017 sui vostri apparati informatici pone l'attenzione alle seguenti problemi ancora in essere e che dovranno essere risolti:

1) **Incontro formativo**: per il personale con data da definire per l'aggiornamento sulle novità e sulle misure minime da intraprendere nel corso dell'anno.

AZIONI DI MANUTENZIONE SINORA INTRAPRESE

1) GESTIONE DISPOSITIVO DI SALVATAGGIO (COMPRESSO E CRIPTATO) PRESSO VOSTRO ISTITUTO CON CONTROLLO REMOTO PERIODICO (SETTIMANALE) DOCUMENTATO.
2) ESECUZIONE DI FILE DISASTER RECOVERY CON PROVA ANNUALE DI RIPRISTINO INTEGRALE DEL SISTEMA OPERATIVO SERVER.
3) CONTROLLO ACCESSI AL SERVER MEDIANTE VERIFICA PERIODICA DEI FILE DI LOG RELATIVI ALL'AMMINISTRATORE DI DOMINIO E COPIA SEMESTRALE SU UNITA' DI SALVATAGGIO.
4) VERIFICA FUZIONI BASE RELATIVE A TUTTI I COMPUTER E UTENTI DELLA RETE QUALI ACCESSO AL DOMINIO TRAMITE ADEGUATA AUTENTICAZIONE.

TALE DOCUMENTO VA ALLEGATO AL DOCUMENTO PROGRAMMATICO DELLA SICUREZZA IN ESSERE COME PARTE INTEGRALE DELLO STESSO.

in fede

Fabio Cavallo