ISTITUTO TECNICO TECNOLOGICO STATALE
"SILVANO FEDI – ENRICO FERMI"

Via Panconi, 14 - 51100 - PISTOIA (ITALIA) Tel. +39 0573 37211 FAX.+39 0573 372121
www.ittfedifermi.gov.it pttf01000r@istruzione.it posta@ittfedifermi.gov.it pttf01000r@pec.istruzione.it
Cod.Fisc.:80007710470 Cod.Mec.:PTTF01000R (serale: PTTF010506) Cod.Fatturazione Elettronica: UFBJA8

Prot. 5733/A33 Pistoia, 23/12/2017

Agli atti

Oggetto: Misure minime di sicurezza ICT per le pubbliche amministrazioni

VISTE le "Misure minime di sicurezza ICT per le pubbliche amministrazioni" di cui alla circolare AGID 18 aprile 2017, n. 2/2017;

VISTO l'art.17 del codice dell'Amministrazione digitale;

VISTA la nota MIUR.AOODGCASIS.REGISTRO UFFICIALE(U).0003015.20-12-2017, che individua nel livello minimo quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme e che questo livello può ritenersi sufficiente per gli istituti scolastici;

VISTA la Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 che definisce le misure relative al livello minimo;

CONSIDERATO che i servizi WEB sono affidati ad Argo Software srl;

VISTA la Policy Argo Software srl in materia di protezione e disponibilità dei dati relativi ai servizi web ricevuta in data 22 dicembre 2017;

VISTO l'incarico di Nomina del Responsabile esterno del trattamento (art. 29 del D.Lgs. n. 196/2003*)* a Argo Software srl del 22 dicembre 2017 prot. 5733/A33 ;

IL DIRIGENTE SCOLASTICO

Adotta il modulo di implementazione delle misure minime di sicurezza riportato di seguito, incaricando per la sua attuazione come responsabile il Prof. Valerio Gabbani:

ABSC 1 (CSC 1): INVENTARIO DEI DISPOSITIVI AUTORIZZATI E NON AUTORIZZATI

Gestire attivamente tutti i dispositivi hardware sulla rete (tracciandoli, inventariandoli e mantenendo aggiornato l'inventario) in modo che l'accesso sia dato solo ai dispositivi autorizzati, mentre i dispositivi non autorizzati e non gestiti siano individuati e sia loro impedito l'accesso

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Realizzazione di un archivio delle risorse attive.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati	L'aggiornamento avverrà quando saranno aggiunte nuove risorse

				in rete.	
1	4	1	M	Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.	**T**ali dati sono inseriti nell'archivio delle risorse attive di cui al punto 1.1.1

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	Realizzazione di un elenco dei software utilizzati su ogni macchina.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Periodicamente saranno realizzate dei controlli per verificare che non siano stati installati software non previsti nell'elenco di cui al punto 2.1.1.

ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	I S.O. saranno configurati con le impostazioni di default e con due utenti base definiti: Amministratore (Privilegi alti con possibilità di intervenire sulla configurazione del S.O.) e Utente (Privilegi limitati all'utilizzo dei sw e divieto di accesso alla modifica del S.O.). L'accesso all'utente Amministratore sarà consentito con credenziali riservate solo ai tecnici e al referente responsabile; in casi particolari anche agli altri docenti, ma solo per motivi giustificati e concertati con il referente ed i tecnici, previa autorizzazione del Dirigente.
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	I Sistemi saranno configurati con le impostazioni predeterminate e concertate fra i docenti. Avranno due utenti base definiti: Amministratore (Privilegi alti con possibilità di intervento sulle installazioni/disinstallazioni dei software e

					con possibilità di intervenire sulla configurazione del S.O.) e Utente (Privilegi limitati all'utilizzo dei sw e divieto di accesso alla modifica del S.O.). L'accesso all'utente Amministratore sarà consentito con credenziali riservate solo ai tecnici e al referente responsabile; in casi particolari anche agli altri docenti, ma solo per motivi giustificati e concertati con il referente ed i tecnici, previa autorizzazione del Dirigente. Tutti i sistemi utilizzeranno sistemi anitvirus integrati nei relativi S.O.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Nel caso in cui un dispositivo risulti compromesso sarà ripristinato alla configurazione standard
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le postazioni, in generale, non prevedono particolari installazioni, per cui in caso di necessità saranno riformattate e successivamente saranno installati i software necessari. Per talune, ritenute più critiche, vengono fatte delle immagini ad-hoc per eventuali ripristini e queste sono conservate su HD esterni, mantenuti distaccati dai PC ed in luogo sicuro
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Tutte le operazioni di amministrazione remota saranno svolte solo attraverso mezzi di connessioni protetti e sicuri. Infatti, Argo utilizza programma teamsystem

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni	Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo dei dispositivo

				delle vulnerabilità più critiche.	
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	I software di ricerca delle vulnerabilità sono regolarmente aggiornati.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni sono configurati per avvenire in automatico
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non vi sono sistemi separati dalla rete, in particolare air-gapped
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio.	Nel caso fossero riscontrati dei problemi, questi saranno risolti attraverso l'installazione di patch o ripristinando il dispositivo.
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Sono state adottate tutte le precauzioni per abbassare al minimo il rischio di sicurezza di ciascun dispositivo utilizzato dall'amministrazione
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Il pericolo è molto basso avendo già previsto che ogni dispositivo si aggiorni automaticamente applicando in tal modo anche le eventuali patch di sicurezza.

ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Per quanto riguarda i sistemi installati negli uffici, si sta procedendo a verificare che l'accesso ai dispositivi da parte degli utenti non avvenga con accessi amministratore e, ove lo fosse, a convertire l'utenza in una non amministrativa.

					Per quanto riguarda i laboratori didattici, che operano su reti isolate e comunque con rischi obiettivamente minori, per ragioni di studio e di apprendimento, sono mantenuti accessi amministratore anche per altri gruppi di utenti che però hanno raggiunto adeguate competenze.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'accesso amministratore ai dispositivi sarà utilizzato solo per operazioni di manutenzione.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Realizzazione di un elenco degli utenti amministratore. Ogni dispositivo avrà una sola utenza amministratore. Talvolta, tale utenza sarà associata al *team* dei tecnici referenti.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Dopo l'installazione di un nuovo dispositivo sarà cambiata la password di default dell'utente amministratore.
5	7	1	M	Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).	Le password utilizzate per le utenze amministratore sono lunghe almeno 14 caratteri e non banali
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le password per le utenze amministratore saranno periodicamente aggiornate
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Le password per le utenze amministrative non saranno riutilizzate a breve distanza di tempo
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Si assicura che c'è la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili	Tutte le utenze amministrative hanno come utente un referente. Talvolta, tale utenza sarà associata al *team* dei tecnici referenti.

				ad una sola persona.	
5	10	3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Le utenze amministrative anonime saranno utilizzate solo per situazioni di emergenza.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate in un luogo sicuro
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano per l'accesso certificati digitali

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE -> DEFENDER

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico.	Su tutti i dispositivi sono installati sistemi atti a rilevare la presenza e bloccare l'esecuzione di malware e sono aggiornati automaticamente
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Ogni dispositivo ha attivo un Firewall
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Per quanto riguarda gli uffici di segreteria, non è consentito l'uso di dispositivi esterni nella rete amministrativa Per quanto riguarda i laboratori didattici, che operano su reti isolate e comunque con rischi obiettivamente minori, per ragioni di studio e di apprendimento, sono mantenuti l'impiego e la connessione alla rete di dispositivi personale degli studenti (BYOD)
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Disattivata l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili su tutti i sistemi Windows 10; da completare per gli altri

8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Disattivata l'esecuzione automatica dei contenuti dinamici presenti nei file.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Disattivata l'apertura automatica dei messaggi di posta elettronica.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Disattivata l'anteprima automatica dei contenuti dei file.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Al momento della connessione di supporti rimovibili sarà eseguita automaticamente una scansione anti-malware
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	Filtrato il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, attraverso l'impiego di strumenti antispam
8	9	2	M	Filtrare il contenuto del traffico web.	Al momento in cui saranno reperite adeguate risorse economiche, sarà installato un proxy server che garantisca il filtraggio del contenuto del traffico web, suddividendo le reti fra segreteria e laboratori.
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	Bloccata nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	I dispositivi operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei	I dispositivi operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto

				supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	I dispositivi operano in con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
13	1	1	M	Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica	I dispositivi operano in con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Bloccato il traffico da e verso url presenti nella blacklist implementata sul Firewall.

Il Dirigente Scolastico
Paolo Bernardi