

	<p align="center">ISTITUTO COMPRENSIVO Alessandro MANZONI Corso Marconi, 28 - 10125 Torino (TO) Tel. 011/669 9446 - fax. 011/ 669 0069 TOIC81900C@istruzione.it - toic81900c@pec.istruzione.it Sito: www.toicmanzoni.gov.it Codice Fiscale 97602020014 Conto corrente postale 18604108 IBAN IT71Q0760101000000018604108</p>	
---	---	---

Prot. n. 8381/VI.11 del 29/11/2017

IL DIRIGENTE SCOLASTICO

- VISTO l'art. 17 del C.A.D. vigente;
- VISTO l'incarico del responsabile alla transizione digitale prot. n. 8379/VI.11 del 29/12/2017;
- VISTA la circolare M.I.U.R. riferita alle misure minime di sicurezza ICT per le pubbliche amministrazioni prot. n. 3015/AOODGCASIS del 20/12/2017;
- VISTA la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017;
- VISTA l'esigenza di compilare il modello di implementazione;

APPROVA

Il seguente modello di implementazione:

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	È stato redatto un inventario di tutti i dispositivi attivi dell'istituto
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	NON disponibile
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con	Non disponibile

				allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Implementabile tramite il firewall installato
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Attuato sulla rete uffici attraverso il firewall
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Controllato ed eseguito periodicamente
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Si, le macchine possono essere collegate solo previa registrazione di MAC e IP in inventario
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Non disponibile
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.	Si, le macchine possono essere collegate solo previa registrazione di MAC e IP in inventario
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	Al momento presente non realizzato
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	Attuato mediante memorizzazione dell'indirizzo MAC
1	5	1	A	Installare un'autenticazione a livello di rete via 802.1x per limitare e controllare quali dispositivi possono essere connessi alla rete. L'802.1x deve essere correlato ai dati dell'inventario per distinguere i sistemi autorizzati da quelli non autorizzati.	Non disponibile
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Non disponibile

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.	Sulla rete didattica l'installazione di nuovi software è consentita soltanto a personale qualificato o all'amministratore di sistema. Sulla rete uffici nuovi software o aggiornamenti dei programmi presenti sono installati esclusivamente dall'amministratore di sistema dopo verifica della tipologia e della funzionalità.
2	2	1	S	Implementare una "whitelist" delle applicazioni autorizzate, bloccando l'esecuzione del software non incluso nella lista. La "whitelist" può essere molto ampia per includere i software più diffusi.	Implementabile, ma al momento non attuato
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un piccolo numero di programmi per funzionare), la "whitelist" può essere più mirata. Quando si proteggono i sistemi con software personalizzati che può essere difficile inserire nella "whitelist", ricorrere al punto ABSC 2.4.1 (isolando il software personalizzato in un sistema operativo virtuale).	Non attuato
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Non attuato
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Tutti i dispositivi sono protetti con antivirus e software che rimuovono automaticamente eventuali installazioni non autorizzate (DeepFreeze)
2	3	2	S	Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop.	Eseguito con verifiche periodiche
2	3	3	A	Installare strumenti automatici d'inventario del software che registrino anche la versione del sistema operativo utilizzato nonché le applicazioni installate, le varie versioni ed il livello di patch.	Non disponibile
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per	Non attuato

				isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	
--	--	--	--	--	--

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.	Nella rete didattica le macchine sono protette da software di ripristino all'avvio Nella rete uffici tutte le macchine sono protette da password e hanno un antivirus installato.
3	1	2	S	Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate.	Applicato sulla rete uffici
3	1	3	A	Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco.	Applicato sui server
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Le macchine omogenee per tipo e sistema operativo hanno delle configurazioni standardizzate.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Il sistema DeepFreeze provvede automaticamente al ripristino della configurazione in caso di alterazioni
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	La configurazione standard viene modificata su autorizzazione del dirigente e dell'amministratore di sistema

3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Sono conservate su partizione nascosta non accessibile
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	N.A.
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).	L'amministrazione remota viene eseguita con apposito software che garantisce la protezione della connessione (Teamviewer). Le credenziali per l'accesso da remoto sono in possesso esclusivamente dell'amministratore di rete
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	Non applicato
3	5	2	A	Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert.	N.A.
3	5	3	A	Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica.	N.A.
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	N.A.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	N.A.
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	N.A.

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

ABSC_ID	Livello	Descrizione	Modalità di implementazione
4	1	Ad ogni modifica significativa della configurazione eseguire	In caso di modifiche si procede alla riconfigurazione dei

				la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	firewall e ad una scansione completa dei sistemi
4	1	2	S	Eeguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Applicato con attenzione focalizzata sulla rete uffici
4	1	3	A	Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common ConfigurationEnumeration Project).	N.A.
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	N.A.
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	N.A.
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	N.A.
4	3	1	S	Eeguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione.	N.A.
4	3	2	S	Vincolare l'origine delle scansioni di vulnerabilità a specifiche macchine o indirizzi IP, assicurando che solo il personale autorizzato abbia accesso a tale interfaccia e la utilizzi propriamente.	Attuato
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Attuato prima di ogni scansione
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità.	N.A.

				Utilizzandole per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	I dispositivi sono configurati per l'aggiornamento automatico del Sistema operativo
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.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	N.a.
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.	Attuato
4	7	2	S	Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio.	Attuato periodicamente
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.).	In fase di realizzazione
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.	Attuato
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	N.A.

4	10	1	S	Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio.	N.A.
---	----	---	---	---	------

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.	Solo l'amministratore di rete dispone di un'utenza con il privilegio di amministratore di dominio. Per quanto riguarda il gestionale di segreteria: I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD). Il sistema AxiosCloud consente le medesime funzionalità.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'accesso alle utenze amministrative è limitato al minimo indispensabile. È installato sui server un software per la registrazione degli accessi e il monitoraggio delle attività. Per quanto riguarda il gestionale di segreteria: I prodotti Axios registrano in automatico ogni accesso effettuato al sistema. Il sistema AxiosCloud possiede un log puntuale di tutte le operazioni effettuate e consente l'accesso allo stesso a qualsiasi richiesta proveniente dall'utente o dalle autorità preposte
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Attuato Per quanto riguarda il gestionale di segreteria: Vedi punto 5.1.1M Anche per AxiosCloud vedi punto 5.1.1M
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	È installato sui server un software per la registrazione degli accessi e il monitoraggio delle attività. Per quanto riguarda il gestionale di segreteria: I prodotti Axios registrano su tabella di log ogni singola operazione effettuata sui dati. La conservazione di tale log dipende dallo spazio presente sul disco del server della scuola e dalle impostazioni fornite dalla scuola stessa sulla grandezza massima

					del file di LOG. Il LOG gestito da AxiosCloud viene storicizzato ogni 3 mesi e collocato in stato di READONLY. Dopo 12 mesi viene cancellato
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'inventario è presente. Per quanto riguarda il gestionale di segreteria: Tramite la gestione utenti di Axios è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso. AxiosCloud consente in ogni istante, da parte dell'amministratore di sistema, di verificare lo status delle utente.
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	N.A.
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.	Le credenziali vengono sostituite prima dell'inserimento in rete.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Per quanto riguarda il gestionale di segreteria: Vedi punto 5.1.4.A L'aggiunta o la soppressione di un'utenza amministrativa sono operazioni che vengono svolte sul DB e quindi regolarmente registrate nel file di LOG. Anche in AxiosCloud l'operazione viene regolarmente tracciata all'interno del file LOG.
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	N.A.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	N.A.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	N.A.
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori	N.A.

				può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi.	
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).	<p>Le password devono rispettare i requisiti di complessità imposti.</p> <p>Per quanto riguarda il gestionale di segreteria: Axios consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi fornite:</p> <ol style="list-style-type: none"> 1. Verifica o meno del doppio accesso 2. Inserimento data generale di scadenza password 3. Numero di gg massimi per la validità del codice di accesso 4. Numero massimo di gg da ultimo accesso per consentire ancora lo stesso 5. Lunghezza minima del codice di accesso (in questo caso 14) 6. Numero minimo dei caratteri minuscoli 7. Numero minimo dei caratteri maiuscoli 8. Numero minimo dei caratteri numerici 9. Numero minimo dei caratteri speciali <p>In AxiosCloud verranno a breve implementate le stesse funzioni</p>
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Per quanto riguarda il gestionale di segreteria: I parametri definiti in Axios al punto precedente (5.7.1.M) consentono di effettuare questo controllo in automatico impedendo di fatto l'utilizzo di credenziali deboli.
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Per le password viene imposta una scadenza trimestrale o semestrale in funzione del grado di criticità. Le password non possono essere ripetute nel tempo Per quanto riguarda il gestionale di segreteria: Vedi parametri indicati nel punto 5.7.1.M
5	7	4	M	Impedire che credenziali già utilizzate possano essere	Non è possibile riutilizzare password precedentemente

				riutilizzate a breve distanza di tempo (password history).	utilizzate. Per quanto riguarda il gestionale di segreteria: Axios gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza. In AxiosCloud sarà a breve implementata la medesima funzione
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Attuato
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Attuato
5	8	1	S	Non consentire l'accesso diretto ai sistemi con le utenze amministrative, obbligando gli amministratori ad accedere con un'utenza normale e successivamente eseguire come utente privilegiato i singoli comandi.	Per quanto riguarda il gestionale di segreteria: Axios consente, per le funzioni particolarmente delicate, di inserire un ulteriore codice di accesso. L'utente quindi dopo aver effettuato il login dovrà inserire anche un ulteriore codice di accesso per poter effettuare la funzione scelta
5	9	1	S	Per le operazioni che richiedono privilegi gli amministratori debbono utilizzare macchine dedicate, collocate su una rete logicamente dedicata, isolata rispetto a Internet. Tali macchine non possono essere utilizzate per altre attività.	N.A.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	La distinzione è assicurata nella configurazione del server Per quanto riguarda il gestionale di segreteria: La gestione degli amministratori rispetto alle normali utenze viene fatta, in Axios, tramite la gestione dei livelli (1-9 9=amministratore) e le tipologie di accesso per ogni utente/funzione (5.1.1M)
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Le utenze sono univocamente legate al personale in servizio. Per quanto riguarda il gestionale di segreteria: In Axios, ad ogni utenze, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi Anche in AxiosCloud le utenze di accesso sono legate a precise anagrafiche presenti nel sistema

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 credenziali sono disponibili solo per il personale autorizzato e per l'amministratore di sistema.
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	Per le macchine a dominio sono usate le utenze di dominio e non quelle locali
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le password delle singole utenze sono custodite in busta chiusa in cassaforte. Alle password hanno accesso soltanto l'amministratore di sistema, il DS e il direttore sga. Per quanto riguarda il gestionale di segreteria: Per quanto concerne i prodotti Axios tali credenziali sono gestite all'interno della base dati, l'accesso alla stessa è consentito solo tramite i programmi Axios e quindi secondo le regole di sicurezza enunciate in questo documento. Anche per AxiosCloud vale lo stesso principio con l'aggiunta che la base dati non è in alcun modo accessibile a nessuno se non tramite programmi Axios e quindi secondo le regole indicate nel presente documento.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	N.A.

ABSC 8 (CSC 8): DIFESA CONTRO I MALWARE

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.	Presenti
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Presenti
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un	In attivazione

				repository centrale (syslog) dove sono stabilmente archiviati.	
8	2	1	S	Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione.	Strumenti modificabili soltanto dall'amministratore di sistema
8	2	2	S	È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale.	Attuabile
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Attuato
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Nella rete uffici non è consentito l'utilizzo di dispositivi "aggiuntivi" a meno che non siano prima stati censiti nell'apposito inventario, memorizzandone indirizzi MAC e IP
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Attuato
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Attuato
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Attuabile
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	Attuato dai firewall
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Attuato tramite antivirus
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	N.A.

8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Attuato
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Attuato
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Attuato
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Attuato
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Attuato
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.	Attuato
8	9	2	M	Filtrare il contenuto del traffico web.	Attuato
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).	Attuato
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Attuato
8	11	1	S	Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate.	Attuabile

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.	Il backup è effettuato quotidianamente. Il log dell'operazione è inviato a mezzo mail alla scuola e all'amministratore di sistema
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare	Attuato

				il sistema operativo, le applicazioni software e la parte dati.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Sono presenti diversi set di backup, per garantire la massima flessibilità
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Attuato con cadenza semestrale
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Il dispositivo di back up è in posizione nascosta nella rete e fisicamente protetto
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.	Le copie vengono duplicate su dispositivi rimovibili

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	In fase di realizzazione: le cartelle contenenti i dati rilevanti saranno cifrate sia sul server che sulle copie di salvataggio in via di implementazione. In una seconda fase i dati rilevanti saranno memorizzati soltanto sul cloud del fornitore del software di segreteria e accessibili soltanto al D.S.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	N.A.
13	3	1	A	Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di	Attuato dal firewall

				informazioni.	
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro.	N.A.
13	5	1	A	Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti.	N.A.
13	5	2	A	Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi.	N.A.
13	6	1	A	Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	N.A.
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	N.A.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	N.A.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Attuato dal firewall
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	N.A.

IL DIRIGENTE SCOLASTICO
dott. Barbato Vetrano
firma autografa sostituita a mezzo stampa,
ex art.3, c.2, D. Lgs 39/93