



ISTITUTO COMPRESIVO "F. DE SANCTIS"

Via Peraine 82010 Moiano BN ☎ Segreteria 0823711653 - ☎ fax 0823711653 - Dirigenza 0823712998
e-mail: bnic83800c@istruzione.it PEC: bnic83800c@pec.istruzione.it sito web: www.icmoiano.gov.it
Codice Fiscale: 92029230627 – Codice Univoco dell'ufficio: UF90A9



Agli Atti

IL DIRIGENTE SCOLASTICO

- VISTO** il D.Lgs 165/2001;
VISTA la circolare AGID n. 2 del 18/04/2017
VISTO il D.Lgs 82/2005 (Codice dell'Amministrazione Digitale)
VISTO il D. Lgs 179/2016
VISTA la Nota MIUR n. 3015 del 20/12/2017 avente ad oggetto "Misure minime di sicurezza ICT per le pubbliche amministrazioni".
VISTA la Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 (Misure Minime di Sicurezza Ict Per Le Pubbliche Amministrazioni) in particolare le indicazioni sulle misure minime.
VISTE le dichiarazioni sulle misure minime di sicurezza ICT garantite, prodotte del gestore esterno dei dati della scuola (AXIOS prot.3489/E VI.1 del 21/12/17 e dalla ditta cui è affidato l'incarico di assistenza (SARDIELLO Salvatore prot. 3513/E VI.1 del 28/12/17

ADOPTA

con il presente documento le **misure minime** di sicurezza ICT per contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informatici, ai sensi dell'art. 3 del D. Lgs 82/2015;

Alla data odierna, si rileva quanto di seguito:

1. Il sistema della rete informatica dell'Istituto è distinto in due specifici segmenti di rete: rete didattica e rete di segreteria.
2. Le reti esistenti sono indipendenti e fisicamente separate:
 - Rete di segreteria (con wi-fi) della SEDE centrale di Moiano - via Peraine
 - Reti didattiche (con wi-fi) dei plessi di Moiano - via Peraine e via Della valle, di Luzzano - via San Vito, di Bucciano - via Provinciale.
3. Il segmento didattico della rete informatica presenta un rischio molto basso poiché le informazioni che transitano sono solo didattiche, non sono presenti dati sensibili poiché inerenti a ricerche e applicativi didattici, senza alcun riferimento a situazioni o persone reali.
4. La rete di segreteria tratta dati più complessi a rischio medio.
5. Le misure di sicurezza prevedono, pertanto, la separazione fisica e software dei due segmenti di rete (didattica e di segreteria).
6. La rete di segreteria e i relativi dispositivi sono dotati di password personalizzate e rispondenti agli standard di sicurezza; è attivo un firewall su ogni macchina e un antivirus sempre attivo.
7. Per quanto concerne la protezione fisica dei dispositivi, gli stessi sono posizionati in un ambiente fisicamente protetto.
8. Il router destinato alla segreteria non fornisce servizio wi-fi.
9. Ognuna delle postazioni di lavoro della segreteria è affidata ad un operatore con rapporto 1:1 e a gestione esclusiva.
10. Ogni laboratorio informatico è affidato ad un responsabile di laboratorio.
11. Il supporto al Dirigente scolastico è fornito dal DSGA per il segmento Ufficio e dai responsabili dall'Animatore digitale, individuato per le competenze informatiche possedute.
12. Il primo controllo di conformità dei livelli minimi di sicurezza dei segmenti della rete informatica dell'ufficio di segreteria è riportato nell'allegato modello di implementazione al quale si rinvia e che costituisce parte integrante del seguente documento.

IL DIRIGENTE SCOLASTICO
Prof.ssa Vanda Lidia Franca DENZA

Firmato in originale - Prof.ssa Vanda Lidia Franca DENZA

Firma autografa sostituita a mezzo stampa ai sensi dell'art. 3 comma 2 decreto legislativo 39/93)

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	Realizzato un inventario delle risorse attive.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'aggiornamento avverrà quando saranno aggiunte nuove risorse Azione: Aggiornare l'elenco delle risorse quando si inserirà un nuovo dispositivo utilizzato dall'amministrazione che risulti essere connesso alla rete
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati 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.	I dati sono inseriti nell'inventario delle risorse attive di cui al punto 1.1.1
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.	
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.	
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.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

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.	Realizzato un elenco per i computer degli uffici di segreteria Azione: Fare un elenco dei software utilizzati su ogni macchina utilizzata per la didattica.
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.	
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).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
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. Azione: Nuovi software installati, se necessari all'amministrazione, comportano l'aggiornamento dell'elenco al punto 2.1.1. che va firmato digitalmente. I precedenti documenti vanno comunque conservati, perché certificano le misure intraprese nel tempo per garantire i minimi di sicurezza.
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.	
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.	
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per 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.	Le configurazioni standard sono quelle già previste dai Sistemi Operativi che si ritengono sufficienti a garantire un livello di sicurezza adeguato per la rete didattica. Per la rete di segreteria si prevede oltre a quanto detto al punto precedente un antivirus per la navigazione in rete. Sono utilizzate copie immagine conservate come descritto al punto 3.3.1 e 3.3.2.
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.	
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.	
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Vedi 3.1.1.
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 con le immagini conservate come descritto al punto 3.3.1 e 3.3.2.
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	

3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Le immagini di installazione standard sono state memorizzate su hard disk esterni e conservati in luogo sicuro.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Gli hard disk esterni sono conservati in luogo sicuro e sono a disposizione del solo personale autorizzato.
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 sono già svolte solo attraverso mezzi di connessioni protetti e sicuri Azione: Chi svolge manutenzione ai dispositivi o che offre assistenza ai software installati, nel caso di accesso remoto utilizza solo protocolli sicuri e criptati.
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.	
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.	
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.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

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 delle vulnerabilità più critiche.	Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo del dispositivo Azione: Effettuare scansioni manuali con Software Antivirus ad ogni aggiornamento significativo (es. Service Pack o Fix di sicurezza) o almeno una volta all'anno.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
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 and Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	

4	3	1	S	Eseguire 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.	
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.	
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 Azione: Verificare che il software Antivirus abbia attivato l'aggiornamento automatico.
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. 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.	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.	I dispositivi air-gapped sono connessi solo nella rete didattica essendo la rete wi-fi di segreteria bloccata.
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.	
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 saranno riscontrati dei problemi questi saranno risolti attraverso l'installazione di patch o ripristinando il dispositivo.
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.	
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 Azione: Garantire che siano state attivate tutte le azioni elencate in questo Vademecum.
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. Azione: Nessuna
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.	
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.	

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.	Si sta procedendo a verificare che l'accesso ai dispositivi da parte degli utenti non avvenga con accessi amministrativi e ove lo fosse a convertire l'utenza in una non amministrativa. I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di

					<p>indicare la tipologia di accesso possibile (CRUD).</p> <p>Il sistema Axios Cloud consente le medesime funzionalità.</p> <p>Azione: Attivarsi affinché gli account utilizzati per accedere al dispositivo non siano di tipo amministrativo. Nel caso lo fossero questi vanno cambiati con accessi di livello più basso.</p>
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	<p>Non è necessario registrare gli accessi nella rete di segreteria poiché vi è un rapporto 1:1 tra operatore e dispositivo.</p> <p>La rete didattica non presenta tale necessità.</p> <p>I prodotti Axios registrano in automatico ogni accesso effettuato al sistema.</p> <p>Il sistema Axios Cloud 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</p> <p>Azione: Come specificato in risposta</p>
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	<p>Ogni dispositivo ha una sola utenza amministrativa; le password sono incluse in un elenco depositato in cassaforte e messo a disposizione solo al personale addetto alla manutenzione dei dispositivi.</p> <p>Tramite la gestione utenti di Axios è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso.</p> <p>Axios Cloud consente in ogni istante, da parte dell'amministratore di sistema, di verificare lo status delle utenze.</p> <p>Azione: Sarà verificato che le password siano non banali e di almeno 14 caratteri di lunghezza. In caso contrario le stesse saranno modificate perché siano conformi agli standard di sicurezza previsti.</p>
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
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	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
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 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>Si controllerà che le password utilizzate per le utenze amministrative siano lunghe almeno 14 caratteri e non banali</p> <p>Axios consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi fornite:</p> <p>1. Verifica o meno del doppio accesso</p>

					<p>2. Inserimento data generale di scadenza password</p> <p>3. Numero di gg massimi per la validità del codice di accesso</p> <p>4. Numero massimo di gg da ultimo accesso per consentire ancora lo stesso</p> <p>5. Lunghezza minima del codice di accesso (in questo caso 14)</p> <p>6. Numero minimo dei caratteri minuscoli</p> <p>7. Numero minimo dei caratteri maiuscoli</p> <p>8. Numero minimo dei caratteri numerici</p> <p>9. Numero minimo dei caratteri speciali</p> <p>In Axios Cloud verranno a breve implementate le stesse funzioni</p> <p>Azione: Vedi azione punto 5.2.1</p>
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Le password per le utenze amministrative saranno periodicamente aggiornate Azione: Il sistema di autenticazione sarà configurato per obbligare tutti gli utenti al cambio password ogni 6 mesi.
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. Axios gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza. In Axios Cloud sarà a breve implementata la medesima funzione Azione: Garantire che le password per le utenze amministrative siano sempre diverse tra loro.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
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.	
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.	
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Si assicurerà la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori. 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) Azione: Sarà garantita se implementata l'azione 5.1.1
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Tutti i dispositivi di segreteria sono nominativi e riconducibili ad una sola persona. In Axios, ad ogni utenze, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi Anche in Axios Cloud 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'immutabilità di chi ne fa uso.	Le utenze amministrative anonime saranno utilizzate solo per situazioni di emergenza. Azione: Come specificato in risposta
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).	
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative sono conservate in un luogo sicuro 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 Axios Cloud 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. Azione: Vedi azione 5.2.1
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. Azione: Nessuna, visto che nessuna scuole dovrebbe avere questo tipo di accesso

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.	Su tutti i dispositivi sono installati sistemi atti a rilevare la presenza e bloccare l'esecuzione di malware e sono aggiornati automaticamente Azione: Vedi azione 2.1.1
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i PC di segreteria è attivato il firewall dell'antivirus. Sui PC della didattica è attivato il firewall che fornisce il Sistema Operativo
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un 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.	
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.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Non è consentito l'uso di dispositivi esterni nella rete amministrativa.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
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.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
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.	

8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
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 Azione: Come specificato in risposta
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. Azione: Come specificato in risposta
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Disattivata l'apertura automatica dei messaggi di posta elettronica. Azione: Come specificato in risposta
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Disattivata l'anteprima automatica dei contenuti dei file. Azione: Come specificato in risposta
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 Azione: Come specificato in risposta è una azione che compiono in automatico la maggior parte degli antivirus
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 antisipam.	La scuola utilizza il servizio di posta elettronica ministeriale e certificata(PEC) che include il filtraggio richiesto. Azione: Per i client locali l'antivirus installato dispone di filtro antisipam che protegge il programma di gestione della posta elettronica
8	9	2	M	Filtrare il contenuto del traffico web.	La scuola utilizza il servizio proxy gratuito di filtraggio web OPENDNS, che consente di innalzare il servizio di sicurezza senza costi per l'amministrazione.
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 Azione: Vedi azione 8.9.2
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
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.	

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 software che gestiscono dati da proteggere richiedono automaticamente le copie di backup pena il blocco delle funzioni. Le copie sono generalmente prodotte il sabato Il programma Axios prevede un sistema automatico e non presidiato di copie del proprio DB presente localmente sul server della scuola. Il sistema prevede inoltre l'invio automatico a tre indirizzi mail e/o a tre numeri di cellulare, di un messaggio sull'esito dell'esecuzione delle copie. Il sistema di backup Axios prevede anche la possibilità di effettuare un backup non solo della base dati ma anche di una specifica

					<p>cartella condivisa sul server della scuola stessa e tutte le sue sottocartelle.</p> <p>Axios Cloud effettua</p> <ul style="list-style-type: none"> - Backup del logo delle transazioni ogni 30 minuti - Backup completo ogni giorno alle 2.00 circa <p>Retention dei backup 8/10 gg</p> <p>Azione: Nessuna, la nota del MIUR richiede che i fornitori di tali servizi compilino l'Allegato 2, sarebbe auspicabile mandare una richiesta in tal senso al fornitore allegando la nota MIUR e l'Allegato 2.</p>
10	1	2	A	Per assicurare la capacità di recupero di un sistema dal proprio backup, le procedure di backup devono riguardare 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.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	
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.	<p>Il backup del server interno è effettuato sull'HD e su pen drive, che sono fisicamente custodite in luoghi diversi.</p> <p>I dispositivi che operano con applicativi che memorizzano i dati sul cloud non necessitano di essere implementati.</p> <p>Il backup effettuato da Axios è un file ZIP criptato che può essere ripristinato solo dalla scuola che lo ha Generato.</p> <p>Questo consente di rimanere a norma anche con l'utilizzo di Backup Cloud di Axios.</p> <p>Axios Cloud consente l'accesso ai dati solo ai legittimi proprietari degli stessi. Tutte le transazioni Axios Cloud sono cifrate e protette da protocollo HTTPS</p> <p>Azione: Nessuna</p>
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.	<p>Si veda il punto 10.3.1.</p> <p>Vedi quanto indicato nel punto 10.1.3.A, in particolare è possibile effettuare una copia su un disco esterno, ad esempio, e poi isolare quest'ultimo dal sistema semplicemente scollegando il cavo dal server.</p> <p>I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery</p>

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	Per i dispositivi che operano con applicativi che memorizzano i dati sul cloud non è necessario implementare tale punto; per gli altri non è necessario attuare nessuna azione. Azione: Nessuna
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
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 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.	
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.	
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.	
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.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
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 presso la sede centrale. Azione: Si procederà al blocco dei dispositivi presenti nelle altre sedi.
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.	

LEGENDA

 DISPOSITIVI LOCALI

 SOFTWARE LOCALE

 SOFTWARE CLOUD