

## ALLEGATO 2 - Modulo implementazione Misure Minime

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
<b>1</b>	<b>1</b>	<b>1</b>	<b>M</b>	<b>Implementare un inventario delle risorse attive correlato a quello ABSC 1.4</b>	Realizzato un archivio delle risorse attive. Documento/conservato presso gli uffici di segreteria (Ufficio DSGA), ed elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio. Si sta valutando la possibilità di censire tutti i dispositivi personali dei docenti che accedono tramite rete dell'istituto al Registro elettronico. Il censimento avverrà tramite richiesta scritta tramite apposito modulo di richiesta.
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.	
<b>1</b>	<b>3</b>	<b>1</b>	<b>M</b>	<b>Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.</b>	L'elenco di cui alla misura 1.1.1 L'aggiornamento avverrà quando saranno aggiunte nuove risorse. L'aggiornamento dell'elenco è a carico degli Amministratori di Sistema/incaricati del DS.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
<b>1</b>	<b>4</b>	<b>1</b>	<b>M</b>	<b>Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP.</b>	Realizzato, tali dati inseriti nell'archivio 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	<b>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.</b>	Realizzato elenco conservato presso gli uffici di segreteria (Ufficio DSGA) L'aggiornamento dell'elenco dei software è a carico degli Amministratori di Sistema/incaricato del Dirigente Scolastico. Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata agli Amministratori di Sistema, che ne verificano la reale esigenza ed eventualmente provvedono affinché sia installato, come pure che venga aggiornato l'elenco. E' stata fatta comunicazione per iscritto a tutti i dipendenti di non installare alcun software se non preventivamente autorizzati (vedi 5.1.1)
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.	E' in fase di studio una soluzione per permettere la gestione delle whitelist compatibilmente con le risorse economiche dell' Istituto.

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	<b>Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.</b>	<p>Gli Amministratori di Sistema/incaricati del DS eseguono periodicamente la verifica del software installato su ciascun dispositivo e comparano il risultato con l'elenco di cui al punto 2.1.1.</p> <p>Eventuale software installato che non risulti nell'elenco viene segnalato agli Amministratori di Sistema/incaricati del DS, che provvedono affinché venga rimosso o, se valutato necessario, a che venga inserito nell'elenco.</p> <p>La scansione per il controllo dei software installati nei dispositivi dell'amministrazione avverrà con cadenza annuale o a necessità dell'amministrazione.</p>
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	<b>Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.</b>	<p>Gli Amministratori di Sistema/incaricati del DS hanno definito e documentato le configurazioni sicure standard per ciascun sistema operativo utilizzato.</p> <p>Le postazioni interessate dal presente punto sono quelle di segreteria e degli uffici di dirigenza che sono dotate di reindirizzamento sul server delle cartelle dei file/documenti ad accesso controllato in base all'utenza di accesso.</p> <p>La disponibilità e l'integrità dei file/documenti sono garantiti da sistema di backup dal server centrale su NAS esterno posto in luogo diverso da quello del server. Tutti gli eseguibili dei software e le procedure di installazione sono salvate e replicate su server e nas e sono ad accesso esclusivo degli Amministratori di Sistema/incaricati del DS. (vedi 3.3.1 e 3.3.2).</p> <p>Le postazioni sono configurate in modalità client su Active directory. Il DB dei software sono centralizzate su server e replicati su NAS non accessibile dalle postazioni. I server utilizzano tecnologia di Virtualizzazione e vengono eseguiti backup sia de i file/documenti che delle intere macchine virtuali, garantendo la possibilità di ripristino dell'intera infrastruttura anche in caso di rottura del server centrale.</p> <p>In caso di danneggiamento del client viene attivata la reinstallazione del sistema operativo e dei software necessari tramite eseguibili a disposizione nel file server. Le configurazioni ed i dati non necessitano di ripristini in quanto centralizzati su server.</p> <p>Tale documentazione è conservata presso Ufficio di Segreteria (Ufficio DSGA). Le postazioni sono dotate di sistemi antivirus e firewall software e vengono aggiornati in automatico, dai produttori, con attività automatiche.</p>
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	<b>Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.</b>	Vedi 3.1.1. Effettuare la configurazione tramite domain controller attraverso active directory
3	2	2	M	<b>Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.</b>	Nel caso in cui un dispositivo risulti compromesso sarà ripristinato alla configurazione standard Attualmente sono implementati i sistemi di backup brevemente elencati al punto 3.1.1.
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	<b>Le immagini d'installazione devono essere memorizzate offline.</b>	LE postazioni non prevedono particolari installazioni, per cui in caso di necessità saranno riformattate e successivamente saranno installati i software necessari. Tale misura non viene garantita, in quanto il sistema è interamente virtualizzato sul principale Domain Controller mediante HyperVisor. L'eventuale ripristino verrà dunque garantito dal backup e dalle repliche, non da immagini d'installazione.
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	I software e gli eseguibili per l'installazione sono conservati in cassaforte chiusa a chiave, su supporti idonei (CD, pennetta usb) sono comunque software standard reperibile anche dal sito del produttori (AXIOS, Agenzia entrate, INPS, etc.).
3	4	1	M	<b>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).</b>	Per attività di gestione effettuate da reti esterne alla rete dell'Istituto vengono utilizzate connessioni VPN o comunque criptate con software dedicati.

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	<b>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.</b>	Attualmente non vengono eseguite le scansioni dei sistemi come disposto dal punto 4.1.1. Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo del dispositivo Sarà inoltre avviata una analisi e valutazione di possibili soluzioni in outsourcing o tramite software da acquistare in base al sistema operativo dell'istituto compatibilmente con i limiti di spesa.
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 ed 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	<b>Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.</b>	Riferimento al punto 4.1.1. In fase di studio per l'implementazione.
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	<b>Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.</b>	Attualmente vengono regolarmente installati automaticamente gli aggiornamenti dei sistemi operativi e le patch a cadenza mensile. Per i sistemi per cui non esiste la possibilità di un automatismo e le patch vengono installate manualmente. L'applicazione delle patch di vulnerabilità è schedulata dagli Amministratori di Sistema Per i seguenti sistemi non esiste la possibilità di un automatismo

					e quindi le patch vengono installate manualmente: - Axios
4	5	2	M	<b>Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.</b>	Sono state date disposizioni agli Amministratori di Sistema/utilizzatori dei dispositivi assegnati dall'istituto di controllare ed aggiornare manualmente periodicamente i sistemi non raggiungibili via rete. Sono state date disposizioni ai possessori di smartphone, tablet o notebook di proprietà dell'ente di accettare gli aggiornamenti proposti automaticamente dal sistema.
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	<b>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.</b>	Riferimento al punto 4.1.1. In fase di studio ed implementazione compatibilmente con i limiti di spesa .Sono state comunque date disposizioni agli Amministratori di Sistema/incaricato del DS di verificare la risoluzione delle vulnerabilità tramite 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	<b>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.).</b>	Sono state adottate tutte le precauzioni per abbassare al minimo il rischio di sicurezza di ciascun dispositivo utilizzato dall'amministrazione.
4	8	2	M	<b>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.</b>	Vedi 4.8.1. In fase di studio ed implementazione compatibilmente con i limiti di spesa. Comunque già il pericolo è molto basso avendo già previsto che ogni dispositivo si arrorni automaticamente applicando in tale modo anche le eventuali patch di sicurezza.
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	<b>Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.</b>	<p>A causa della mancanza di personale tecnico adibito a questa attività (aggiornamenti software delle procedure e dei programmi) si è reso necessario assegnare privilegi di amministrazioni su utente di dominio locale. E' allo studio la possibilità di modificare i privilegi degli utenti locali da amministratori a user in modo da assegnare i privilegi di amministratore solo agli amministratori di sistema espressamente nominati da parte dell'ente.</p> <p>I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD).</p> <p>Il sistema Axios Cloud consente le medesime funzionalità. I privilegi di amministrazione per tablet sono assegnati al soggetto al quale l'apparato è dato in dotazione dato che devono avere la possibilità di accettare in autonomia gli aggiornamenti di sicurezza.</p>
5	1	2	M	<b>Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.</b>	<p>L'accesso amministrativo ai dispositivi sarà utilizzato solo per operazioni di manutenzione.</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. E' attivato il log di sistema per registrare gli accessi come amministratore su PC, server, apparati di rete.</p> <p>Attualmente le operazioni di accesso e disconnessione svolte dalle utenze amministrative, sono registrate nei file di LOG</p>

					<p>standard del SO Windows Server 2012 R2. Gli accessi ai software locali di segreteria (software Axios) sono salvati nel log dentro ala database</p> <p>I file LOG, così come gli altri dati , sono memorizzati a cadenze regolari mediante backup su NAS di rete accessibile solo agli utenti amministratori di sistema.</p> <p>(vedi anche 3.4.1).</p>
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	<p>Vedi punto 5.1.1M</p> <p>Anche per Axios Cloud vedi punto 5.1.1.M</p>
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	<p>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.</p> <p>Il LOG gestito da Axios Cloud viene storicizzato ogni 3 mesi e collocato in stato di READONLY. Dopo 12 mesi viene cancellato</p>
5	2	1	M	<b>Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.</b>	<p>Oni dispositivo avrà una sola utenza da amministratore.</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 utente.</p> <p>L'inventario è contenuto in Active Directory e gli Amministratori sono autorizzati a compiere le operazioni di loro competenza.</p> <p>(vedi 5.11.1).</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	<b>Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.</b>	<p>Agli amministratori di sistema/incaricati del DS sono state impartite adeguate istruzioni al riguardo, tra cui il cambio password di default delle eventuali utenze da amministratore dei nuovi dispositivi.</p>
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	<p>Vedi punto 5.1.4.A L'aggiunta o la soppressione di un'utenza amministrativa sono operazioni che vengono svolte sul DB e</p>

					quindi regolarmente registrate nel file di LOG. Anche in Axios Cloud l'operazione viene regolarmente tracciata all'interno del file LOG.
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	<b>Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).</b>	<p>Le password per l'accesso alle postazioni con l'utenza amministratore sono lunghe almeno 14 caratteri e non banali. 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"> <li>1. Verifica o meno del doppio accesso</li> <li>2. Inserimento data generale di scadenza password</li> <li>3. Numero di gg massimi per la validità del codice di accesso</li> <li>4. Numero massimo di gg da ultimo accesso per consentire ancora lo stesso</li> <li>5. Lunghezza minima del codice di accesso (in questo caso 14)</li> <li>6. Numero minimo dei caratteri minuscoli</li> <li>7. Numero minimo dei caratteri maiuscoli</li> <li>8. Numero minimo dei caratteri numerici</li> <li>9. Numero minimo dei caratteri speciali</li> </ol> <p>In Axios Cloud verranno a breve implementate le stesse funzioni Il sistema di autenticazione per tutti gli utenti obbliga all'utilizzo di password di autenticazioni "forti". "almeno 8 caratteri di cui uno speciale + 1 numero + una maiuscola"</p>
5	7	2	S	<b>Impedire che per le utenze amministrative vengano utilizzate</b>	I parametri definiti in Axios al punto precedente (5.7.1.M)

				<b>credenziali deboli.</b>	consentono di effettuare questo controllo in automatico impedendo di fatto l'utilizzo di credenziali deboli.
5	7	3	M	<b>Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)</b>	Vedi parametri indicati nel punto 5.7.1.M Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password ogni 3 mesi.
5	7	4	M	<b>Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).</b>	Le utenze delle postazioni 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 Il sistema di autenticazione è configurato per impedire il riutilizzo a breve distanza di tempo delle credenziali già utilizzate in precedenza.
5	7	5	S	<b>Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.</b>	
5	7	6	S	<b>Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.</b>	
5	8	1	S	<b>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.</b>	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.	
5	10	1	M	<b>Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.</b>	Gestione utenze separate 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) Agli amministratori di sistema sono state impartite adeguate

					istruzioni al riguardo. Utilizzando il servizio Active Directory fornito dal SO Windows Server 2012 R2 tale completa distinzione tra le utenze privilegiate e non privilegiate degli amministratori viene correttamente implementata.
5	10	2	M	<b>Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.</b>	Tutte le utenze amministrative hanno come utente: administrator 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 Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	10	3	M	<b>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.</b>	Le utenze amministrative anonime saranno utilizzate solo per situazioni di emergenza. Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
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	<b>Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.</b>	Per le utenze delle postazioni le credenziali amministrative sono conservate in 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. Le credenziali amministrative non personali sono conservate in busta chiusa e sigillata in cassaforte presso ufficio di segreteria (UFFICIO DSGA)
5	11	2	M	<b>Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.</b>	Non si utilizzano certificati digitali per l'autenticazione delle utenze amministrative.

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione
8	1	1	M	<b>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.</b>	Su tutti i PC, portatili e server è installato un antivirus con aggiornamento automatico.
8	1	2	M	<b>Installare su tutti i dispositivi firewall ed IPS personali.</b>	Su tutti i PC, portatili e server Windows è attivato il firewall fornito dal 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	<b>Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.</b>	E' stata data disposizione, ai dipendenti, di limitare l'uso di dispositivi esterni a quelli necessari per le attività scolastiche.
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	<b>Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.</b>	Disattivata l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.
8	7	2	M	<b>Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.</b>	Disattivata l'esecuzione automatica dei contenuti dinamici presenti nei file.
8	7	3	M	<b>Disattivare l'apertura automatica dei messaggi di posta elettronica.</b>	Disattivata l'apertura automatica dei messaggi di posta elettronica.
8	7	4	M	<b>Disattivare l'anteprima automatica dei contenuti dei file.</b>	Disattivata l'anteprima automatica dei contenuti dei file.
8	8	1	M	<b>Eeguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.</b>	Al momento della connessione di supporti rimovibili sarà eseguita automaticamente una scansione anti-malware ed è stato comunicato ai dipendenti le corrette attività da fare in caso di collegamento di una unità rimovibile
8	9	1	M	<b>Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antisipam.</b>	Filtrato il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, attraverso l'impiego di strumenti antisipam
8	9	2	M	<b>Filtrare il contenuto del traffico web.</b>	Il sistema antivirus in dotazione all'Istituto prevede la funzione di controllo del traffico WEB. Si sta valutando la possibilità di acquistare/implementare servizi firewall dedicati con content-filtering in base alle disponibilità economiche. Sono state date disposizioni agli amministratori di sistema di configurare il software antivirus delle postazioni di lavoro in tal senso.
8	9	3	M	<b>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).</b>	Il sistema antivirus in dotazione all'Istituto prevede la funzione di controllo del traffico WEB. Bloccata nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa
8	10	1	S	<b>Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.</b>	Il sistema antivirus in dotazione all'Istituto prevede la funzione di controllo del traffico WEB.
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	<b>Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.</b>	<p>Il programma Axios prevede un sistema automatico e non presidiato di copie del proprio DB presente localmente sul server della scuola.</p> <p>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.</p> <p>Il sistema di backup Axios prevede anche la possibilità di effettuare un backup non solo della base dati ma anche di una specifica cartella condivisa sul server della scuola stessa e tutte le sue sottocartelle.</p> <p>Axios Cloud effettua</p> <ul style="list-style-type: none"> <li>- Backup del log delle transazioni ogni 30 minuti</li> <li>- Backup completo ogni giorno alle 2.00 circa</li> <li>- Retention dei backup 8/10 gg</li> </ul> <p>Giornalmente vengono effettuate copie di backup di tutte le Macchine Virtuali installate sugli host, comprensive quindi di tutti i dati in esse contenuti, inoltre viene fatto backup (copia intera) delle cartelle dei documenti e dei db. La copia viene effettuata con salvataggio su dispositivo NAS conservato all'interno dell'Istituto.</p>
10	1	2	A	<b>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.</b>	<p>Per quanto concerne Axios il sistema di backup effettua il salvataggio della base dati. L'installazione dei programmi è possibile in qualsiasi momento dal sito internet di Axios, così come l'eventuale ripristino del motore di database utilizzato (Sybase ver. 8.0.2.4495)</p> <p>Axios Cloud oltre ad esser dotato di un sistema di backup con retention di 8/10gg dei dati ed un sistema di retention di 2/4 gg delle immagini dell'intera infrastruttura e configurato con un sistema di DR Real Time che consente il ripristino di un subset depotenziato dell'infrastruttura madre entro 24/48 ore dal Fault completo del sistema principale garantendo, quindi, la continuità di servizio con uno SLA del 98.98 % circa</p>
10	1	3	A	<b>Effettuare backup multipli con strumenti diversi per</b>	Axios consente alle scuole di poter effettuare, nella medesima



				<b>contrastare possibili malfunzionamenti nella fase di restore.</b>	<p>sessione di copie ed in modo completamente automatico, oltre alla copia sul disco del server, anche una copia su unità fisica esterna e, qualora la scuola abbia acquistato il servizio, anche un backup cloud che garantisce l'assoluta salvaguardia e recuperabilità dei dati.</p> <p>I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery</p>
<b>10</b>	<b>2</b>	<b>1</b>	<b>S</b>	<b>Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.</b>	<p>Axios effettua una verifica al termine della creazione del file compresso contenente le copie. La simulazione del ripristino dei dati è comunque buona pratica da adottare con frequenza almeno mensile</p>
<b>10</b>	<b>3</b>	<b>1</b>	<b>M</b>	<b>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.</b>	<p>Il backup dei file e delle cartelle viene salvato all'interno di supporti custoditi in ambienti ad accesso riservato e controllato. Il backup effettuato da Axios è un file ZIP criptato che può essere ripristinato solo dalla scuola che lo ha generato. Questo consente di rimanere a norma anche con l'utilizzo di Backup Cloud di Axios. 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>E' stata data disposizione agli amministratori di sistema di configurare in tal senso il sistema di backup.</p> <p>Più specificatamente...</p> <p>La copia delle cartelle dei dati vengono copiate dentro al nas (ogni 7 backup, uno per ogni giorno, vengono cancellati i più vecchi), le copie. Il DB del database Axios viene crittografato e copiato sul NAS. Il Backup del database Axios oltre che essere copiato sul NAS (dopo essere stato crittografato).</p>
<b>10</b>	<b>4</b>	<b>1</b>	<b>M</b>	<b>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.</b>	<p>Vedi quanto indicato nel punto 10.1.3.A, in particolare viene effettuata 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> <p>E' stata data disposizione agli amministratori di sistema di</p>

					<p>configurare in tal senso il sistema di backup.          Più specificatamente il dispositivi NAS non è raggiungibili direttamente dagli utenti, ma esclusivamente dal software di Backup, soltanto nel momento di eseguire la replica dei contenuti. Anche la copia delle macchine virtuali viene replicata all'interno del Nas. A cadenza impostata dall'amministratore di sistema, viene fatta ulteriore copia da NA sas un disco esterno sostituito ogni settimana e riposto in cassaforte.</p>
--	--	--	--	--	--

### ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione
<b>13</b>	<b>1</b>	<b>1</b>	<b>M</b>	<b>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</b>	L'analisi dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL). I dati all'interno del software axios sono crittografati. Sono crittografate anche le copie di backup create dal sistema.
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.	
<b>13</b>	<b>8</b>	<b>1</b>	<b>M</b>	<b>Bloccare il traffico da e verso url presenti in una blacklist.</b>	Vedi misura 8.9.2
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.	