ISTITUTO COMPRENSIVO "P. STRANEO"
VIA P. SACCO, 11 - 15121 ALESSANDRIA
TEL. 0131/346280 - FAX 0131/346315
C. F. 96034380061 Cod. Univoco PA: UFU2HQ
e-mail: alic815008@istruzione.it PEC: alic815008@pec.istruzione.it

Prot. 7064/C17 Alessandria, 29/12/2017

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 SicurezzaICT per Le Pubbliche Amministrazioni) in particolare le indicazioni sulle misure minime.

ADOTTA
le seguenti MISURE MINIME DI SICUREZZA ICT per l'I.C. STRANEO DI ALESSANDRIA

Art.1
Adozione misure minime di sicurezza ICT per le pubbliche amministrazioni – I.C. STRANEO

Le **misure minime** di sicurezza ICT di seguito riportate vendono adottate dall'I.C. Straneo di Alessandria al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informatici, ai sensi dell'art. 3 del D. Lgs 82/2015.

Art. 2
Struttura e architettura della rete

La rete dell'IC "Straneo" di Alessandria è strutturata in due segmenti:

- **segmento della didattica** - *quattro reti indipendenti e fisicamente separate nei seguenti plessi:*
  - rete didattica presso scuola secondaria di I grado Straneo
  - rete didattica presso scuola primaria Morbelli
  - rete didattica presso scuola primaria Caduti per la Libertà
  - rete didattica presso scuola primaria di Borgoratto
- **segmento della segreteria**
  LAN (Local Area Network) topologia a stella, tipologia Client-Server e software applicativi (Axios) condivisi per la gestione dei dati (i dati degli alunni e del personale sono archiviati in cloud).

Art.3

-Valutazione del rischio, misure di prevenzione e rinvio-

Il segmento della didattica presenta un rischio molto basso poiché le informazioni che transitano sono solo didattiche, non sono presenti dati sensibili poiché inerenti ricerche e applicativi didattici, senza alcun riferimento a situazioni o persone reali.
La rete di segreteria tratta dati più complessi a rischio medio a tal fine le misure di sicurezza prevedono la separazione fisica e software dei due segmenti di rete (didattica e di segreteria).
La rete di segreteria e i relativi dispositivi sono dotati di password personalizzate e rispondenti agli standard di sicurezza.
Inoltre è presente un firewall hardware (Watchguard) per tutta la LAN e su ogni macchina è attivo un antivirus (Symantec Endpoint Protection).
Per quanto concerne la protezione fisica dei dispositivi, gli stessi sono posizionati in un ambiente fisicamente protetto. Il router destinato alla segreteria non fornisce servizio wi-fi.
Ognuna delle postazioni di lavoro della segreteria è affidata ad un operatore con rapporto 1:1 e a gestione esclusiva.
Il dirigente è supportato dall'amministratore di sistema e dagli operatori di segreteria.
Per la didattica, ogni laboratorio informatico (con ciò si intende la strumentazione informatica di ogni plesso) è affidata ad un responsabile di laboratorio.

Le misure sono descritte nell'allegato 1 "Modulo implementazione Misure Minime, Standard e Avanzato*"* al quale si rinvia.

Il Dirigente Scolastico
Dott.ssa Maria Paola Minetti
(documento firmato digitalmente)

ALLEGATO 1 - Modulo implementazione Misure (Minime – Standard – Avanzate)

SI RITIENE SIANO SUFFICIENTI LE MISURE LIVELLO M – NOTA MIUR 3015 DEL 20/12/2017

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**	L'inventario è disponibile presso l'ufficio economato ed è costantemente aggiornato. L'inventario elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio ed è strutturato nel modo seguente: • codice identificativo assegnato all'apparato; • descrizione breve del tipo di dispositivo; I seguenti dati : • indirizzo IP (statico) • collocazione e persona alla quale è assegnato; • nome postazione; sono conservati in una cartella riservata all'Amministratore di Sistema (AS)
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Implementato tramite WORD/EXCEL
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	La scannerizzazione e il discovery degli indirizzi IP e del Mac è realizzabile mediante il software freeware Advanced IP Scanner 2.5
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Il router traccia gli IP assegnati ai dispositivi mediante l'associazione dell'IP al MAC Address
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	E' installato un server DHCP utilizzato dall'amministratore di sistema solo in casi eccezionali. Tutti gli IP dei client sono statici.
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Ved 1.2.1 Non è necessario né utile inventariare gli strumenti del amministratore di sistema che utilizza in casi eccezionali per controlli/manutenzione
1	**3**	**1**	**M**	**Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.**	L'elenco di cui alla misura 1.1.1 è aggiornato. L'aggiornamento dell'elenco è a carico dell' amministratore di sistema.

1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Non necessario ai fini istituzionali.
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.**	Vedi 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.	Vedi punto 1.1.1 Relativamente all'assegnazione di IP dinamici da parte del router (DHCP) si rimanda a quanto esposto nei punti 1.1.4. e 1.2.1.
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.	Tutti gli strumenti di proprietà della scuola sono inventariati come detto al punto 1.1.1.
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.	Non implementabile per le ragioni di cui a 1.2.2

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.**	L'aggiornamento dell'elenco dei software è a carico dell'amministratore di sistema. Sono state date direttive al personale di non installare alcun software diverso. Eventuali nuovi software sono installati esclusivamente dall'amministratore dopo verifica della tipologia e della funzionalità. Le abilitazioni all'installazione del software sono stati concessi solamente agli amministratori di sistema (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.	Il Firewall è impostato con i software ritenuti utili e affidabili prioritariamente per la segreteria.
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 si ritiene necessario.
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.**	L'amministratore di sistema esegue periodicamente la verifica del software installato su ciascun dispositivo e compara il risultato con l'elenco di cui al punto 2.1.1. Eventuale software installato che non risulti nell'elenco viene segnalato al Responsabile della transizione Digitale, che provvede affinché venga rimosso o, se valutato necessario, a che venga inserito nell'elenco.

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.	Inventario di cui al punto 2.1.1
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 sono necessari considerato che non vi sono elementi di rischio a ciò connessi. I dispositivi della segreteria sono monitorati direttamente dal responsabile della transizione digitale.
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.	IL rischio è basso pertanto non è previsto.

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. Tutti i client sono protetti da password e hanno un antivirus/firewall installato. 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.	• rimozione di software non necessario dal sistema; • disabilitazione di servizi e moduli non necessari (msconfig); • installazione di antivitus/firewall compatibile con i software esistenti; • all'applicazione di permessi restrittivi sui file; • all'applicazione di policy per la complessità delle password; • rimozione degli utenti non necessari;
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.**	Eseguito dall'amministratore di sistema.
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	I cambiamenti sono autorizzati dal responsabile della transizione al digitale.
3	**3**	**1**	**M**	**Le immagini d'installazione devono essere memorizzate offline.**	Sono conservate in partizioni riservate del HD. L'eventuale ripristino da crash del database e dei dati è riparabile mediante il ripristino da unità NAS (backup a giorni alterni)
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Non previsto per le ragioni 3.1.1
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).**	Le connessioni con le reti ministeriali avvengono con protocolli sicuri (https, ecc…). In caso di necessità vengono abilitate temporaneamente connessioni attraverso protocolli sicuri e disabilitate al termine dell'intervento.
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.	Il controllo avviene mediante il software antivirus ed Anti-Malware per rilevare la presenza eventuale di *malicious software* (malware appunto).
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.	L'antivirus prevede l'alert automatico poiché è sempre attivo e ogni nuovo file eseguibile è scannerizzato in tempo reale.
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.	Il software antivirus e anti-malware centralizzato è 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.	Ogni operatore di segreteria monitora costantemente mediante il sistema antivirus ogni eventuale attacco esterno.
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Tramite software antivirus e anti-malware Symantec Endpoint Protection

3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Le configurazioni sono standard e quindi non si ritiene necessario attivare ulteriori sistemi di ripristino rispetto a quelli previsti dal S.O. proprietario in uso (punti di ripristino a cadenza regolare).

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.**	Si utilizza il software antivirus e anti-malware Symantec Endpoint Protection per la scansione vulnerabilità.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Scansione su tutta la rete da parte dell'amministratore di sistema.
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).	Symantec Endpoint Protection
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Symantec Endpoint Protection
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Symantec Endpoint Protection
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Symantec Endpoint Protection
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.	Symantec Endpoint Protection
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.	Le scansioni sono condotte solo sui dispositivi di segreteria e sono eseguite dall'amministratore di sistema.

4	**4**	**1**	**M**	**Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.**	Il software di scansione è aggiornato giornalmente e prima di ciascun utilizzo. Gli antivirus nei client sono configurati per 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	Servizio fornito da Watchguard e Symantec Endpoint Protection.
4	**5**	**1**	**M**	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**	L'applicazione delle patch di vulnerabilità è schedulata da Symantec Endpoint Protection. Qualora l'applicazione automatica delle patch non abbia avuto successo o provochi gravi problemi al funzionamento dei sistemi, sarà necessario bloccare l'attività di patching.
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.	Symantec Endpoint Protection
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.**	Sono state date disposizioni agli operatori di segreteria di verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie saranno attivate le eventuali contromisure.
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.	Gli operatori di segreteria di comune accordo con il responsabile della transizione concorderanno diversi e accettabili livelli 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.).**	Esistono procedure automatizzate di backup per la salvaguardia dei dati residenti in sede.
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.**	Tutte le patch relative a vulnerabilità vengono immediatamente implementate appena disponibili

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.	Vedi 4.8.2 I dati sono in parte delocalizzati, invece, per quelli residenti in sede si eseguono regolari backup.
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.**	I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD). Il sistema Axios Cloud 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.**	I prodotti Axios registrano in automatico ogni accesso effettuato al sistema. 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
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Vedi punto 5.1.1M
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	I prodotti Axios registrano su tabella di log ogni singola operazione effettuata sui dati. Il LOG gestito da Axios Cloud 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.**	Tramite la gestione utenti di Axios è possibile verificare in qualsiasi momento lo status delle utenze, non ultima la data di ultimo accesso. Axios Cloud 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.	
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.**	

5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	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. 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**	**Quando l'autenticazione a più fattori non è supportata, utilizzare per le utenze amministrative credenziali di elevata robustezza (e.g. almeno 14 caratteri).**	Axios consente di definire una serie di parametri che possono rendere sicure le credenziali di accesso ai propri programmi fornite: 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
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	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).**	Vedi parametri indicati nel punto 5.7.1.M
5	**7**	**4**	**M**	**Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).**	Axios gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza.
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.	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**	**Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.**	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.**	In Axios, ad ogni utenza, è legata la relativa anagrafica del personale gestita all'interno dei programmi stessi
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.	
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.**	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. 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.
5	**11**	**2**	**M**	**Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.**	

ABSC 8 (CSC 8): DIFESE 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 PC e server è installato un antivirus con aggiornamento automatico. Risulta inoltre presente software per il rilievo della presenza di malicious software (Malwarebytes Anti-Malware) con settaggio per l'aggiornamento automatico.
8	**1**	**2**	**M**	**Installare su tutti i dispositivi firewall ed IPS personali.**	Su tutti i PC, portatili e server Windows è attivato il firewall di Windows.
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Non è sempre necessario poiché l'intervento di recupero è immediato.
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.	Confermato.
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.	Come punto 8.1.1
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Come punto 8.1.1
8	**3**	**1**	**M**	**Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.**	Ai dipendenti è stata data disposizione di limitare l'uso di dispositivi esterni a quelli necessari per le attività di segreteria.
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Non applicabile per le ragioni di cui al punto 8.3.1
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.	Symantec Endpoint Protectionoltre ad essere già una funzionalità del sistema operativo Windows.
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Symantec Endpoint Protection e window defender.
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.	L'utilizzo dei software antivirus sono più che sufficienti.
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Non si ritengono necessari anche perchè gli antivirus già svolgono tali azioni.

8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Symantec Endpoint Protection + gestione attraverso la funzionalità del firewall del S.O.
8	**7**	**1**	**M**	**Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.**	E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro.
8	**7**	**2**	**M**	**Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.**	E' stata data disposizione agli di segreteria di configurare in tal senso le postazioni di lavoro.
8	**7**	**3**	**M**	**Disattivare l'apertura automatica dei messaggi di posta elettronica.**	E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro.
8	**7**	**4**	**M**	**Disattivare l'anteprima automatica dei contenuti dei file.**	E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro.
8	**8**	**1**	**M**	**Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.**	E' stata data disposizione agli operatori di segreteria di configurare in tal senso le postazioni di lavoro.
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.**	La scuola utilizza il servizio di posta elettronica ministeriale e certificata(PEC) che include il filtraggio richiesto.
8	**9**	**2**	**M**	**Filtrare il contenuto del traffico web.**	Il firewall Watchguard e Symantec Endpoint Protection includono funzioni di filtraggio.
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).**	Il firewall Watchguard e Symantec Endpoint Protection includono funzioni di filtraggio.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Non necessario il livello di controllo.
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.	Non necessario il livello di controllo.

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.**	Axios Cloud effettua - Backup del logo delle transazioni ogni 30 minuti - Backup completo ogni giorno alle 2.00 circa - Retention dei backup 8/10 gg
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.	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
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	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.
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 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

10	**4**	**1**	**M**	**Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.**	I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery

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**	L'analisi dei livelli particolari di riservatezza è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è fisicamente controllato e protetto da password.
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Il sistema di cifratura utilizzato è quello previsto dai software in utilizzo sia per i dati in locale che per quelli in cloud.
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.	Gli operatori di segreteria sono stati adeguatamente istruiti in merito.
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.	Si veda il punto 13.2.1
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.	Non necessario data l'architettura di cui all'art.2 del presente atto di adozione.

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.	Non necessario data l'architettura di cui all'art.2 del presente atto di adozione.
13	6	1	A	Implementare strumenti DLP (Data LossPrevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	Non necessario data l'architettura di cui all'art.2 del presente atto di adozione.
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	I software di controllo di cui alla sezione 8 sono più che sufficienti.
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Non necessario data l'architettura di cui all'art.2 del presente atto di adozione.
13	**8**	**1**	**M**	**Bloccare il traffico da e verso url presenti in una blacklist.**	Vedi misura 8.9.2 La misura è implementata nel 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.	Non necessario data l'architettura di cui all'art.2 del presente atto di adozione.