Centro Provinciale Istruzione Adulti (C.P.I.A.)
Caltanissetta/Enna
C.F. 92063460858 - Codice meccanografico: CLMM04200B
Sede amministrativa: Viale Regina Margherita, n. 26 – 93100 Caltanissetta
Tel/Fax: 0934_22131 - C.U.: UF0KQG
p.e.o.: clmm04200b@istruzione.it - p.e.c.: clmm04200b@pec.istruzione.it
sito web: www.cpia-cl-en.gov.it

Caltanissetta, 28.12.2017

Albo on line
Dsga
Atti

IL DIRIGENTE SCOLASTICO

VISTA la circolare AGID n. 2/2017 del 18 aprile 2017 relativa alle Misure minime di sicurezza ICT per le pubbliche amministrazioni

CONSIDERATO che le misure previste devono essere adottate dal responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del codice dell'Amministrazione digitale, oppure, in sua assenza, del dirigente allo scopo designato ;

VISTA la nota MIUR n. 3015 del 20/12/2017;

CONSIDERATO che tali misure devono essere adottate da parte di tutte le pubbliche Amministrazioni entro il 31 dicembre 2017,

ASSUME

Il ruolo di Responsabile della struttura per l'organizzazione, l'innovazione e le tecnologie di cui all'art.17 del codice dell'Amministrazione digitale.

ADOTTA

Le misure minime di sicurezza ICT previste per le pubbliche amministrazioni, provvede alla compilazione del "modulo di implementazione" che, firmato digitalmente, sarà conservato agli atti dalla scuola.
Tale modulo sarà aggiornato in funzione dei cambiamenti e dei miglioramenti conseguiti nel tempo.

Il Dirigente Scolastico
Prof. Giovanni Bevilacqua
Firma autografa sostituita a mezzo stampa ai sensi e per gli effetti dell'art. 3, comma 2 del D.Lgs. 39/93

Know K. Srl
www.knowk.it
info@knowk.it
knowk@pec.knowk.it

Si prega di consegnare il seguente documento
Al Dirigente Scolastico
Al Direttore dei Servizi Generali ed Amministrativi
Al Responsabile della Sicurezza

MISURE MINIME DI SICUREZZA

La circolare AgID del 26 Aprile 2016 in materia di "MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI" deve essere vista come un documento utile a guidare le PA in un processo di conoscenza delle misure di sicurezza e della loro attuazione in base alla struttura delle singole PA.

La nota congiunta MIUR/AgID, spiega, come il documento allegato alla circolare in oggetto e da compilare entro il 31/12/2017, non deve intendersi statico o impositivo, ma uno strumento per valutare la situazione della sicurezza nei sistemi informativi delle scuole e predisporre nel tempo gli adeguamenti necessari. Deve essere quindi visto come una guida alla cultura della sicurezza nelle scuole.

Know K. intende da parte sua, con questa comunicazione, aiutare la compilazione del modello nei capitoli di propria competenza (ABSC 5 ed ABSC 10) delegando alla propria rete la consulenza da dare alle scuole per identificare e catalogare le peculiarità di ognuna.

E' evidente che questo documento, perché generico, non può tenere conto delle singole situazioni che devono essere indicate da ogni singola scuola.

Di seguito i capitoli riguardanti Know K. e cosa, a nostro giudizio, dovrebbero contenere come informazioni.

All'interno della tabella "ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE" sono indicate ovviamente tutte le informazioni concernenti il portale KK. E' importante ricordare come all'interno di tale tabella debbano essere indicati "Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi."

Come privilegi di amministratore non si intende solo l'amministratore del Portale KK. ma qualsiasi altra utenza avente tali caratteristiche, dall'amministratore della macchina a quello di rete e del server.

Le indicazioni fornite quindi devono essere integrate con le informazioni circa la gestione delle utenze sopra descritte.

Esistono una serie di programmi free in internet che possono aiutare la scuola nella gestione di tali utenze al fine di rispettare quando indicato nella norma.

Know K. Srl
www.knowk.it
info@knowk.it
knowk@pec.knowk.it

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

ABSC_ID			Livello	D	Modalità di
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.	Il Portale KK. consente, per ogni utente di indicare la tipologia di accesso possibile e le relative funzionalità
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Il Portale KK. possiede un log puntuale di tutti gli accessi effettutati e consente l'accesso allo stesso
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.	Il LOG gestito dal Portale KK. viene storicizzato ogni 15 giorn. Dopo 1 mese viene cancellato
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Il Portale KK. consente, in ogni istante, da parte dell'amministratore del sistema, di verificare le utenze amministrative e lo stato delle stesse
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Il Portale KK. consente, in ogni istante, da parte dell'amministratore del sistema, di verificare le utenze amministrative e lo stato delle stesse
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.	Il Portale KK. consente, in ogni istante, da parte dell'amministratore del sistema, di verificare le utenze amministrative e lo stato delle stesse

Know K. Srl
www.knowk.it
info@knowk.it
knowk@pec.knowk.it

5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Nel Portale KK. verrà implementata questa funzionalità
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Nel Portale KK. verrà implementata questa funzionalità
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Nel Portale KK. verrà implementata questa funzionalità
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.	Nel Portale KK. verrà implementata questa funzionalità
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.	Il Portale KK. distingue l'accesso in base al ruolo assegnato, distinguendo tra amministratori ed utenze non privilegiate
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Nel Portale KK. l'utenza di accesso è legata ad un'anagrafica personale presente nel sistema

Know K. Srl
www.knowk.it
info@knowk.it
knowk@pec.knowk.it

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	D	Modalità di
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Il Portale KK. effettua - Backup del log delle transazioni ogni giorno - Backup completo ogni giorno alle 2.00 circa - Retention dei backup 30 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.	Il Portale KK. oltre ad esser dotato di un sistema di backup con retention di 30gg dei dati ed un sistema di retention di 30 gg delle immagini dell'intera infrastruttura e configurato con un sistema che consente il ripristino dell'infrastruttura madre entro 72 ore dal Fault completo del sistema principale garantendo, quindi, la continuità di servizio con uno SLA del 97.00 % circa
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	I backup del Portale KK. 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.	I backup del Portale KK. sono dump di database ed immagini di sistema, il cui test viene effettuato periodicamente (cadenza trimestrale circa)
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 Portale KK. consente l'accesso ai dati solo ai legittimi proprietari degli stessi. Tutte le transazioni del Portale KK. 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 del Portale KK. sono conformi a tutte le regole attuali per il Disaster Recovery

Si prega di consegnare il seguente documento
Al Dirigente Scolastico
Al Direttore dei Servizi Generali ed Amministrativi
Al Responsabile della Sicurezza

MISURE MINIME DI SICUREZZA

La circolare AgID del 26 Aprile 2016 in materia di "MISURE MINIME DI SICUREZZA ICT PER LE PUBBLICHE AMMINISTRAZIONI" deve essere vista come un documento utile a guidare le PA in un processo di conoscenza delle misure di sicurezza e della loro attuazione in base alla struttura delle singole PA.
Nei prossimi giorni uscirà una nota congiunta MIUR/AgID che spiegherà come il documento allegato alla circolare in oggetto e da compilare entro il 31/12/2017, non deve intendersi statico o impositivo, ma uno strumento per valutare la situazione della sicurezza nei sistemi informativi delle scuole e predisporre nel tempo gli adeguamenti necessari. Deve essere quindi visto come una guida alla cultura della sicurezza nelle scuole.
Axios intende da parte sua, con questa comunicazione, aiutare la compilazione del modello nei capitoli di propria competenza (ABSC 5 ed ABSC 10) delegando alla propria rete la consulenza da dare alle scuole per identificare e catalogare le peculiarità di ognuna.
E' evidente che questo documento, perché generico, non può tenere conto delle singole situazioni che devono essere indicate da ogni singola scuola.
Di seguito i capitoli riguardanti Axios e cosa, a nostro giudizio, dovrebbero contenere come informazioni.
Indicando i pacchetti Axios si intendono tutti i nostri prodotti Windows client/server, con l'indicazione invece di Axios Cloud, tutti i nostri programmi CLOUD (SD, RE e Protocollo)

All'interno della tabella "*ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE*" sono indicate ovviamente tutte le informazioni concernenti i prodotti Axios. E' importante ricordare come all'interno di tale tabella debbano essere indicati "*Regole, processi e strumenti atti ad assicurare il corretto utilizzo delle utenze privilegiate e dei diritti amministrativi.*"
Come privilegi di amministratore non si intende solo l'amministratore dei programmi Axios ma qualsiasi altra utenza avente tali caratteristiche, dall'amministratore della macchina a quello di rete e del server.
Le indicazioni fornite quindi devono essere integrate con le informazioni circa la gestione delle utenze sopra descritte.
Esistono una serie di programmi free in internet che possono aiutare la scuola nella gestione di tali utenze al fine di rispettare quando indicato nella norma.

All'interno della tabella "*ABSC 10 (CSC 10): COPIE DI SICUREZZA*" devono essere indicati "*Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità.*"
Uno degli strumenti più efficaci per garantire la sicurezza delle copie dei dati è sicuramente dato dal poter effettuare un backup su server cloud. Attenzione però perché questi devono in qualche modo essere certificati ed essere locati all'interno della Comunità Europea, in quanto, all'interno della base dati, sono presenti dati sia personali che sensibili.
Non è opportuno quindi utilizzare spazi cloud free, come forniscono molti giganti del WEB in quanto, pur perfettamente funzionanti, non garantiscono sicurezza e locazione geografica dei vostri backup.
Axios propone in questo caso ai propri clienti, al fine di essere tranquilli riguardo ad una procedura di Disaster Recovery, il proprio programma di Backup Cloud, completamente integrato ed automatizzato, che garantisce un elevato standard di sicurezza e protezione oltre ad una collocazione fisica dei server all'interno del territorio nazionale.

Programmi Axios Client/Server (seguire quanto indicato con il colore rosso)

Programmi Axios Cloud (seguire quanto indicato con il colore blue)
I programmi Axios in Cloud, Segreteria Digitale, Registro Elettronico e Protocollo WEB, così come i futuri sviluppi della tecnologia Axios in cloud sono installati e gestiti all'interno del data center di uno dei più grandi fornitori di servizi WEB collocato sul territorio nazionale: Aruba SpA.
Aruba si è dotata della certificazione ISO 27001:2013 e degli altri mezzi e/o strumenti ritenuti idonei a tutelare nella maniera più efficace la sicurezza delle informazioni (fisica, logica, informatica ed organizzativa). Il servizio da noi utilizzato è Server Dedicati, Housing e Colocation ed è certificato **ISO 9001:2008** per la qualità e **ISO 27001:2005** per la sicurezza.

Allegato 2

				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 In Axios Cloud verranno a breve implementate le stesse funzioni
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. In Axios Cloud sarà a breve implementata le medesima funzione
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 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	

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 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 cartella condivisa sul server della scuola stessa e tutte le sue sottocartelle. 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.	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) 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.	Axios consente alle scuole di poter effettuare, nella medesima 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. 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

A2

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	**Rispondere**: Realizzato un archivio delle risorse attive. **Azione** da fare: realizzare un elenco dei dispositivi utilizzati dall'amministrazione in tutti i suoi plessi collegati alla rete dati. L'archivio potrebbe essere così organizzato: Nome PC Collocazione IP Assegnato Applicativi installati
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 operazione 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.	**Rispondere:** 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.	**Rispondere**: Realizzato, tali dati sono inseriti nell'archivio delle risorse attive di cui al punto 1.1.1 **Azione**: Nessuna
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	

					nell'elenco di cui al punto 2.1.1. **Azione**: Periodicamente, non è specificato un minimo, va verificato che non siano installati nuovi software, se questo avvenisse perché necessari all'amministrazione va aggiornato l'elenco al punto 2.1.1. aggiornata la versione del documento e 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.	**Rispondere**: per sistemi desktop e server definire dotazione software standard e criteri di gruppo nel domain controller attraverso l'active directory per gestire le richieste di autenticazione per la sicurezza. **Azione:** definire dotazione software standard e criteri di gruppo nel domain controller attraverso l'active directory per gestire le richieste di autenticazione per la sicurezza.
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	

				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.	**Rispondere**: Saranno garantite delle scansioni di vulnerabilità dopo ogni aggiornamento significativo dei 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 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	

Allegato 2 – Misure minime di sicurezza ICT per le pubbliche amministrazioni - Servizi web Argo

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.	Per quanto attiene ai servizi web Argo: Vengono effettuate copie dei database più volte al giorno, a intervalli regolari, e con modalità differenti (full e incrementali). Le copie vengono mantenute presso i server delle infrastrutture per sette giorni. Quotidianamente una copia full di dati viene riversata in un sistema di storage. L'integrità delle copie di sicurezza nell'operazione di trasmissione verso il sistema di storage è garantita da un sistema di hashing che controlla l'impronta del file di destinazione con quello di origine. Le copie quotidiane vengono mantenuta per un periodo di 2 mesi. Una copia settimanale dei dati viene mantenuta per un periodo di 4 mesi. Una copia mensile dei dati viene mantenuta per un periodo di 6 mesi. Copie degli applicativi vengono eseguite ad ogni rilascio di aggiornamenti.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Per quanto attiene ai servizi web Argo: prove di ripristino dei backup vengono effettuate con cadenza 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.	Per quanto attiene ai servizi web Argo: le copie di sicurezza sono compresse con chiave di cifratura.
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.	Per quanto attiene ai servizi web Argo: tutti i server dell'infrastruttura Argo (application /database/ backup server) sono accessibli esclusivamente dalla rete Argo. La Argo Software si affida esclusivamente a server farm di comprovata affidabilità ed esperienza in materia di sicurezza informatica, e comunque previa verifica delle misure fisiche, logiche e organizzative poste in capo alle infrastrutture informatiche fornite. Ad ogni fornitore è richiesta come requisito la certificazione ISO 27001.

				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.	**Rispondere**: Realizzato **Azione**: Fare un elenco dei software utilizzati su ogni macchina. Non c'è bisogno di elencare quelli di sistema basta precisare la versione del Sistema Operativo, mentre vanno elencati tutti quelli installati compreso l'antivirus. Tra i software installi è indispensabile che ci sia un Antivirus che si aggiorni automaticamente.
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.	**Rispondere:** Periodicamente saranno realizzate dei controlli per verificare che non siano stati installati software non previsti

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.	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. I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery.

				"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. 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.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	

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 Anche per Axios Cloud vedi punto 5.1.1.M
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. La conservazione di tale log dipende dallo spazio presente sul disco del server della scuola e dalle impostazioni fornite dalla scuola stessa sulla grandezza massima del file di LOG. Il LOG gestito da 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. 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,	

Know K. Srl
www.knowk.it
info@knowk.it
knowk@pec.knowk.it

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.	Fare in modo che tali password siano a conoscenza di una sola persona per volta (conservare le password in busta chiusa in cassaforte per emergenze)
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).	Fare in modo che tali password siano a conoscenza di una sola persona per volta (conservare le password in busta chiusa in cassaforte per emergenze)
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali di accesso sono conservate in uan database, pertanto l'accesso agli stessi è consentito solo a personale autorizzato e solo dietro programma Know K., 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.	Il Portale KK. non utilizza certificati digitali

Know K. Srl
www.knowk.it
info@knowk.it
knowk@pec.knowk.it

5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Nel Portale KK. viene tracciata, nel file di log, l'operazione di soppressione di un'utenza amministrative
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Nel Portale KK. quest'operazione viene tracciata, nel file di log.
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Nel Portale KK. quest'operazione viene tracciata, nel file di log.
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Nel Portale KK. quest'operazione viene tracciata, nel file di log.
5	6	1	A	Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli biometria ed altri analoghi sistemi. 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	Nel Portale KK. verrà implementata questa funzionalità
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).	Nel Portale KK. verrà implementata questa funzionalità
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Nel Portale KK. verrà implementata questa funzionalità
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Nel Portale KK. verrà implementata questa funzionalità

Know K. Srl
www.knowk.it
info@knowk.it
knowk@pec.knowk.it

All'interno della tabella "ABSC 10 (CSC 10): COPIE DI SICUREZZA" devono essere indicati "Procedure e strumenti necessari per produrre e mantenere copie di sicurezza delle informazioni critiche, così da consentirne il ripristino in caso di necessità."

Uno degli strumenti più efficaci per garantire la sicurezza delle copie dei dati è sicuramente dato dal poter effettuare un backup su server cloud. Attenzione però perché questi devono in qualche modo essere certificati ed essere locati all'interno della Comunità Europea, in quanto, all'interno della base dati, sono presenti dati sia personali che sensibili. Non è opportuno quindi utilizzare spazi cloud free, come forniscono molti giganti del WEB in quanto, pur perfettamente funzionanti, non garantiscono sicurezza e locazione geografica dei vostri backup.

Know K. utilizza una procedura di backup che, in caso di Disaster Recovery, garantisce un elevato standard di sicurezza e protezione oltre ad una collocazione fisica dei server all'interno del territorio nazionale.

Il Portale KK. e tutti i servizi in cloud offerti, sono installati e gestiti all'interno del data center di uno dei più grandi fornitori di servizi WEB collocato sul territorio nazionale: Aruba Business SpA.

Aruba Business SpA si è dotata della certificazione ISO 27001:2013 e degli altri mezzi e/o strumenti ritenuti idonei a tutelare nella maniera più efficace la sicurezza delle informazioni (fisica, logica, informatica ed organizzativa). Il servizio da noi utilizzato è Server Dedicati, Housing e Colocation ed è certificato ISO 9001:2008 per la qualità e ISO 27001:2005 per la sicurezza.

Nome PC	Collocazione	IP ASSEGNATO	Applicativi installati	Antivirus installato	Sistema Operativo utilizzato
Asus Zenbook	Ufficio Dirigente Scolastico	192.168.1.136	Pacchetto Office 2013	Windows Security E.	Microsft Windows 10
Asus Asuspro	Ufficio Segreteria	192.168.1.178	Axios; Libre Office	----------	Microsoft Windows 10 PRO
Asus Splendid Tryme	Ufficio Segreteria	192.168.1.3	Axios; Argo EmolumentiOffice	Avira Antivirus	Microsoft Windows 10 PRO
Asus HDMI	Ufficio Segreteria	192.168.1.1	Axios; Office;Argo;	Avira Antivirus	Microsft Windows 2007
ASUS HDMI	Ufficio Segreteria	192.168.1.14	Axios; Libre Office;	Avira Antivirus	Microsoft Windows 10 PRO
Asus ASUSPRO	Ufficio Segreteria	192.168.1.122	Libre Office; Axios	----------	Microsoft Windows 10 PRO
Asus HDMI	Ufficio DSGA	10.0.0.1 A 10.0.9.254	Axios; Office; Argo Bilancio	Microsoft Defender	Microsoft Windows 2007Mi

Allegato 2 – Misure minime di sicurezza ICT per le pubbliche amministrazioni - Servizi web Argo

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	Per quanto attiene ai servizi web Argo: La gestione e configurazione dei server è eseguita esclusivamente da personale Argo. Gli addetti alla gestione dei server sono nominati dalla Argo amministratori di sistema. Per quanto riguarda la gestione dei privilegi di amministrazione dei servizi web, la Argo si attiene alle misure prescritte dal Garante della Privacy con Provvedimento del 27 novembre 2008 e succ. modifiche, recante <<Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema>>. Gli accessi ai server e ai servizi di gestione degli stessi sono monitorati. L'accesso da parte degli amministratori viene eseguito sempre attraverso utenze di dominio. Con cadenza mensile viene eseguito il controllo sui log degli accessi degli amministratori di sistema da parte del responsabile della gestione privacy Argo. I log delle operazioni e degli accessi sono marcati temporalmente e archiviati per un periodo di 18 mesi.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	v. ABSC_ID 5.1.1
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	v. ABSC_ID 5.1.1
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	v. ABSC_ID 5.1.1
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	v. ABSC_ID 5.1.1

				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.	**Risposta**: Bloccato il traffico da e verso url presenti nella blacklist implementata sul Firewall. **Azione**: Vedi azione 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.	

				supporti rimuovibili al momento della loro connessione.	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 antispam.	**Risposta:** Filtrato il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, attraverso l'impiego di strumenti antispam **Azione:** Attivare il filtro antispam del programma di gestione della posta elettronica
8	9	2	M	Filtrare il contenuto del traffico web.	**Risposta:** Sarà installato un proxy server che garantisca il filtraggio del contenuto del traffico web **Azione:** La scuola si dovrà dotare di un Proxy Server in grado di filtrare il traffico web, ci sono molte soluzioni gratuite che impiegano vecchi PC (es. IPCOP, Smoothwall, ZeroShell, ect.) e che consentono di alzare il livello 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).	**Risposta:** 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.	**Risposta**: I dispositivi operano con applicativi che memorizzano i dati sul cloud per cui non è necessario implementare tale punto **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

					Azione: Creare in tutte le macchine un utente amministrativo che abbia lo stesso nome utente e sia riconducibile a chi svolge la manutenzione dei dispositivi.
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.	**Rispondere:** 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.	**Risposta:** Le credenziali amministrative sono conservate in un luogo sicuro **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.	**Risposta:** Non si utilizzano per l'accesso certificati digitali **Azione:** Nessuna, visto che nessuna scuole dovrebbe avere questo tipo di accesso

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.	**Risposta:** 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.	**Risposta:** Ogni dispositivo ha attivo un Firewall **Azione:** Attivare, se non lo fosse già, su ciascun dispositivo 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	

				le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	dispositivi da parte degli utenti non avvenga con accessi amministrativi e ove lo fosse a convertire l'utenza in una non amministrativa **Azione**: Attivarsi affinché gli account utilizzati per accedere al dispositivo non siano di di tipo amministrativo. Nel caso lo fossero questi vanno cambiati con accessi di livello più basso.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	**Rispondere:** L'accesso amministrativo ai dispositivi sarà utilizzato solo per operazioni di manutenzione. **Azione**: Come specificato in risposta
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.	**Rispondere:** Ogni dispositivo avrà una sola utenza amministrativa **Azione:** Predisporre un elenco degli utenti amministrativi e relativa password assegnata. Tale elenco dovrà essere custodito in cassaforte e messo a disposizione solo al personale addetto alla manutenzione dei dispositivi. Le password dovranno essere non banali e di almeno 14 caratteri di lunghezza.
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.	**Rispondere:** Dopo l'installazione di un nuovo dispositivo sarà cambiata la password di default dell'utente amministratore. **Azione**: Come specificato in risposta, da effettuare al momento dell'installazione del nuovo dispositivo
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	

				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.	**Rispondere**: 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.	**Rispondere**: Le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni sono configurati per avvenire in automatico **Azione**: Verificare che ogni postazione abbia attivi gli aggiornamenti automatici del sistema e dei software installati
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.	**Se vi fossero dispositivi utilizzati e non connessi alla rete rispondere**: Sarà garantito l'aggiornamento anche ai dispositivi air-gapped. **Azione**: Aggiornare manualmente e periodicamente i dispositivi non connessi alla rete per cui non è possibile impostare l'aggiornamento automatico. **Se non vi fossero dispositivi utilizzati e non connessi alla rete rispondere**: Non vi sono dispositivi air-gapped

				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.	**Rispondere**: effettuare la configurazione tramite domain controller attraverso l'active directory. **Azione:** effettuare la configurazione tramite domain controller attraverso l'active directory.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	**Rispondere:** Nel caso in cui un dispositivo risulti compromesso sarà ripristinato alla configurazione standard **Azione**: Se un virus o qualunque azione malevola infetti la macchina questa va riformatta e portata ai valori standard.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	**Rispondere:** Le postazioni non prevedono particolari installazioni, per cui in caso di necessità saranno riformattate e successivamente saranno installati i software necessari. **Azione:** Nessuna
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
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).	**Rispondere:** Tutte le operazioni di amministrazione remota saranno svolte solo attraverso mezzi di connessioni protetti e sicuri **Azione**: Avvisare chi svolge manutenzione ai dispositivi o che offre assistenza ai software installati, che nel caso di accesso remoto dovrà avvenire solo utilizzando 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	