Misure Minime di sicurezza ICT per le PA

Il presente documento è una implementazione da parte di Easyteam.org del documento ufficiale AgID reperibile al seguente indirizzo:

http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/cert-pa/misure-minime-sicurezza-ict-pubbliche-amministrazioni

Mantenendo gli stessi contenuti del documento originale, aggiunge alcune tabelle per una più facile comprensione e gestione del piano di sicurezza.

Il presente documento, unitamente ai documenti:

- **Manuale di gestione del Protocollo Informatico**
- **Piano di sicurezza informatica, continuità operativa a e di Disaster Recovery (contenuto del documento precedente)**
- **Certificazione Misure Minime Dlgs 196/2003 Allegato B con allegato Piano di gestione dei rischi**
- **Relazione semestrale Amministratore di Sistema**
- **Dichiarazione dell'Amministratore di Sistema sulle modalità e sulle tecniche da lui utilizzate per implementare le procedure richieste dal presente documento**

costituisce pieno adempimento a quanto richiesto da:

- Circolare MIUR 21/11/2017
- Circolare AgID 18/04/2017 n. 2
- Direttiva PCM 01/08/2015

E' importante tenere presente che i documenti citati nell'elenco precedente costituiscono un unico *corpus* e che solo congiuntamente permettono all'Amministrazione di adempiere completamente a quanto richiesto dalle normative.

Acronimi utilizzati nelle Circolari ufficiali e nel resto del presente documento

Sigla	Significato	Note
ABSC	AgID Basic Security Control(s)	Controlli di sicurezza previsti dall'AgID
CSC	Critical Security Control(s)	Controlli di sicurezza critici, ritenuti fondamentali
CSSC	CIS - Critical Security Controls for Effective Cyber Defense	Controlli di sicurezza critici per una protezione funzionale dagli attacchi cibernetici

Livelli di sicurezza utilizzati nel presente documento

Nel documento, per ogni singola implementazione tecnica, è indicato il livello di sicurezza relativo. Le misure previste dal livello minimo devono essere messe in atto quanto prima, poiché ritenute necessarie dall'AgID.

Sigla	Significato	Note
M	Minimo	Livello sotto il quale nessuna amministrazione può scendere: i controlli indicati debbono riguardarsi come **obbligatori**
S	Standard	Base di riferimento per un livello di sicurezza completo. Rappresenta il primo step a cui tendere per la protezione della propria infrastruttura informatica
A	Alto	Obiettivo finale a cui tendere, al completamento del piano di sicurezza

Nel corso del documento sono state evidenziate con diversi colori le singole misure previste, in modo da fornire un veloce colpo d'occhio su quanto sia:

- strettamente necessario: rosso
- da programmare: azzurro
- obiettivo finale: verde

Tempi di implementazione

La tabella proposta dall'AgID è stata integrata con una colonna che permette all'Amministrazione di specificare i tempi di messa in opera di ogni misura di sicurezza.

Sigla	Descrizione
II	Implementazione **Immediata**. Da mettere in atto quanto prima per raggiungere il livello minimo richiesto
ID	Implementazione in itinere, **durante** la validità del piano di sicurezza informatica
IS	Implementazione a **scadenza**, da realizzarsi entro il termine di validità del piano di sicurezza informatica

Note specifiche programmi Axios

I programmi Axios in Cloud, 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 utilizzato da Axios è *Server Dedicati, Housing e Colocation* ed è certificato ISO 9001:2008 per la qualità e ISO 27001:2005 per la sicurezza.

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	L'amministratore di rete fornisce elenco dei server, dei PC e dei dispositivi (stampanti, scanner, NAS, Access Point, switch) presenti nella rete	II
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	L'amministratore di rete installa uno strumento hardware/software che periodicamente controlla i dispositivi presenti in rete	IS
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	L'amministratore di rete installa uno strumento hardware/software che periodicamente controlla i dispositivi presenti in rete	IS
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	L'amministratore di rete installa uno strumento hardware/software che periodicamente controlla i dispositivi presenti in rete	IS
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	L'amministratore di rete attiva i LOG del server DHCP, se presente	IS
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	L'amministratore di rete verifica periodicamente i log e li confronta con i propri elenchi di dispositivi	ID
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'amministratore di rete aggiorna la documentazione	II
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	L'amministratore di rete aggiorna la documentazione	IS
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.	L'amministratore di rete aggiorna la documentazione	II

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.	L'amministratore di rete aggiorna la documentazione	IS
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.	L'amministratore di rete aggiorna la documentazione e verifica periodicamente i log dei dispositivi che hanno utilizzato la rete	IS
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.	L'amministratore di rete verifica che nulle reti WIFI sia presente un sistema di autenticazione Captive Portal basato su account singoli e non su chiave WPA/WPA2 comune	IS
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	L'amministratore verifica l'esistenza (ove possibile) di certificati lato client.	IS

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
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'amministratore di rete aggiorna la documentazione	II
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.	L'amministratore di rete aggiorna la documentazione	IS
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).	L'amministratore di rete aggiorna la documentazione	IS
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	L'amministratore di rete utilizza strumenti hardware/software di checksum sui repository software	IS
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	L'amministratore di rete verifica le applicazioni installate	II
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.	L'amministratore di rete aggiorna la documentazione	IS
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.	L'amministratore di rete predispone su un server apposito degli strumenti per l'analisi delle configurazioni software della rete	IS

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.	L'amministratore di rete verifica se esistono applicazioni di questo tipo e predispone i dovuti accorgimenti di protezione	IS

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	Tempi
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	L'amministratore di rete impartisce istruzioni su come gestire i singoli sistemi operativi e fornisce un manuale contenente le istruzioni sull'utilizzo corretto della rete e delle risorse di rete	II
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.	L'amministratore di rete, all'atto dell'installazione di una nuova postazione, verifica che siano rispettate le procedure di hardening: - eliminazione account non necessari - disabilitazione servizi non necessari - chiusura porte di rete non necessarie	ID
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.	L'amministratore di rete mantiene un archivio aggiornato delle immagini dei sistemi installati	IS
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	L'amministratore di rete redige un documento in cui si definisce la configurazione standard delle workstation della rete	II
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	L'amministratore di rete definisce le procedure di ripristino	II
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	L'amministratore di rete definisce le procedure di ripristino	IS
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	L'amministratore di rete mantiene un archivio aggiornato delle immagini dei sistemi installati	II
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	L'amministratore di rete mantiene un archivio aggiornato delle immagini dei sistemi installati	IS

3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	L'amministratore di rete verifica che su server e workstation siano utilizzati solo strumenti di amministrazione remota che rispettino i protocolli di connessione protetta	II
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.	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
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'amministratore di rete utilizza strumenti di checksum sui repository software	IS
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.	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	L'amministratore di rete utilizza strumenti di checksum sui repository software	IS

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
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.	L'amministratore di rete verifica che siano impostate operazioni pianificate di verifica delle vulnerabilità (Antivirus, antimalware, etc)	II
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	L'amministratore di rete verifica che siano impostate operazioni pianificate di verifica delle vulnerabilità (Antivirus, antimalware, etc)	ID
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).	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	IS
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID
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.	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID
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.	L'amministratore di rete predispone un sistema hardware/software SCAP di monitoraggio	ID

4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici degli strumenti di scansione	II
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	L'amministratore di rete certifica di essere abbonato a un servizio online di informazioni sulla cybersicurezza	ID
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici dei sistemi	II
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.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici dei sistemi e provvede ad aggiornare i sistemi non collegati direttamente alla rete	II
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.	L'amministratore di rete verifica i i log delle attività	ID
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.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici dei sistemi	II
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.	L'amministratore di rete verifica che siano attivi gli aggiornamenti automatici dei sistemi e decide i livelli di rischio in base ai risultati emersi	ID
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.).	L'amministratore di rete stila un elenco delle modalità di gestione dei rischi	II
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.	L'amministratore di rete stila un elenco delle modalità di gestione dei rischi	II

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.	L’amministratore di rete stila un elenco delle modalità di gestione dei rischi	ID
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.	L’amministratore di rete certifica di essere in possesso di ambienti di test su cui valuta l’impatto di prodotti non standard sugli apparati della rete	IS

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
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.	L'amministratore di rete verifica i privilegi degli account utente. I prodotti Axios consentono, per ogni utente ed ogni funzionalità, di indicare la tipologia di accesso possibile (CRUD).	II
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	L'amministratore di rete verifica i privilegi degli account utente. 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	II
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	L'amministratore di rete verifica i privilegi degli account utente. Vedi punto 5.1.1M	ID
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi. 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	ID
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	L'amministratore di rete redige la documentazione della rete. 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.	II

5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	L'amministratore di rete redige la documentazione della rete e la mantiene aggiornata tramite strumenti software	IS
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.	L'amministratore di rete verifica i privilegi degli account utente	II
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi. 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.	ID
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi	IS
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi	IS
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	L'amministratore di rete installa sui server un sistema di controllo dei log degli accessi	IS
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.	L'amministratore di rete verifica le modalità degli accessi amministrativi	IS

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).	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. 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	II
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. 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.	ID
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. Vedi parametri indicati nel punto 5.7.1.M	II
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003. Axios gestisce lo storico password impedendo di fatto che possa essere riutilizzato un codice di accesso già utilizzato in precedenza.	II

5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003	ID
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	L'amministratore di rete verifica che la complessità delle password delle utenze amministrative sia rispondente a quanto richiesto dall'Allegato B del Dlgs 196/2003	ID
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.	L'amministratore di rete verifica le modalità degli accessi amministrativi. 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.	IS
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.	L'amministratore di rete verifica le modalità degli accessi amministrativi	IS
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	L'amministratore di rete verifica le modalità degli accessi amministrativi. 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)	II
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	L'amministratore di rete verifica le modalità degli accessi amministrativi. 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	II
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.	L'amministratore di rete verifica le modalità degli accessi amministrativi	II

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).	L'amministratore di rete verifica le modalità degli accessi amministrativi	ID
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	L'amministratore di rete verifica le modalità degli accessi amministrativi. 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.	II
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	L'amministratore di rete verifica le modalità degli accessi amministrativi	II

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
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.	L'amministratore di rete verifica la presenza di sistemi antivirus e firewall software locali	II
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	L'amministratore di rete verifica la presenza di sistemi antivirus e firewall software locali	II
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	L'amministratore di rete installa e configura un sistema di gestione centralizzata dei log	IS
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.	L'amministratore di rete verifica che gli antivirus locali siano gestibili attraverso un sistema centralizzato	ID
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.	L'amministratore di rete verifica che gli antivirus locali siano gestibili attraverso un sistema centralizzato	ID
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	L'amministratore di rete verifica che gli antivirus locali siano gestibili attraverso un sistema centralizzato	ID
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	L'amministratore di rete verifica l'utilizzo di dispositivi esterni	II
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	L'amministratore di rete verifica l'utilizzo di dispositivi esterni	IS
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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	ID

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'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
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.	L'amministratore di rete predispone adeguate Group Policies sui server di dominio	II
8	9	2	M	Filtrare il contenuto del traffico web.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	II
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).	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	II
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	ID
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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. 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	II
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.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. 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	IS

10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. 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	IS
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. 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.	ID
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.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. 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	II
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.	L'amministratore di rete predispone e mette in atto un piano di backup e disaster recovery adeguato. 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	II

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID			Livello	Descrizione	Modalità di implementazione	Tempi
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'amministratore di rete verifica che i dati siano trattati in conformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	II
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	L'amministratore di rete verifica che i dati siano trattati in conformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	IS
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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS
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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS
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.	L'amministratore di rete verifica che i dati siano trattati in conformità con quanto richiesto dall'Allegato B del Dlgs 196/2003	IS
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.	L'amministratore di rete verifica la presenza di siffatti dispositivi e li include nella lista dei dispositivi autorizzati sulla rete	IS
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.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS

13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	L'amministratore di rete installa e predispone adeguati strumenti hardware/software IDS, DEP, ASLR	IS
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	L'amministratore di rete verifica che il firewall in uso sulla rete permetta le gestione di blacklist e whitelist	II
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.	L'amministratore di rete predispone che i sistemi di copiatura mantengano le regole di controllo sui dati e verifica che i software in uso consentano l'applicazione di tali regole	IS