ISTITUTO COMPRENSIVO "TOMMASONE - ALIGHIERI"
LUCERA (FG)
Piazza Matteotti, 1 - 71036 Lucera
Tel./fax 0881/522662
P.E.C. fgic876009@pec.istruzione.it P.E.O.: fgic876009@istruzione.it
Codice Meccanografco: FGIC876009 Codice Fiscale 91022320716
Sito web: www.tommasone-alighieri.edu.it

Prot. n. (come da segnatura) Lucera, 16.03.2023

## IL DIRIGENTE SCOLASTICO

**VISTO** il D.Lgs 165/2001;

**VISTO** il D.Lgs 82/2005 *(Codice dell'Amministrazione Digitale)*;

**VISTO** il D.Lgs 179/2016;

**VISTA** la circolare AGID n. 2 del 18/04/2017;

**VISTA** la Direttiva del Presidente del Consiglio dei Ministri 1 agosto 2015 (*Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni)*;

**CONSIDERATO i**l Modulo di Implementazione, adottato da questo Istituto con prot. n. AOO10006763/A28 del 28.12.2017;

**CONSIDERATO** il documento "*Policy AXIOS Software*" in materia di protezione e disponibilità dei dati relativi ai servizi web, e archiviato agli atti della Scuola;

**SENTITO** il parere del Responsabile della Transizione digitale, ins. Gennaro Camporeale;

**PRESO ATTO** di quanto dichiarato dal tecnico incaricato della gestione dei sistemi informatici e della manutenzione hardware dell'Istituto;

**VISTA** la delibera n. 121 del Collegio dei docenti, Verbale n.6 del 27 giugno 2020, recante: "*Piano di implementazione – Misure minime di sicurezza ICT per le Pubbliche Amministrazioni*";

**VISTO** il decreto dirigenziale n.49, prot. n.4394/I9 del 10.08.2020, recante: "*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni. Pubblicazione del Modulo di Implementazione di cui all' Allegato 2 della Circolare AgID 2/2017";*

**VISTE** le "*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni. Pubblicazione del Modulo di Implementazione di cui all' Allegato 2 della Circolare AgID 2/2017". Adottate con prot.* 4395/I9 del 10 .08. 2020;

**VISTI** gli esiti delle verifiche effettuate in sede di collegio del 30 giugno 2021 ( Del n. 144) e nel Consiglio di Istituto del 25 maggio 2021 (Del. n. 150);

**VISTI** gli aggiornamenti apportati con Prot. n. 2329 del 16.02.2022 alle "*Misure minime di sicurezza ICT per le Pubbliche Amministrazioni. Pubblicazione del Modulo di Implementazione di cui all' Allegato 2 della Circolare AgID 2/2017". Adottate con prot.* 4395/I9 del 10 .08. 2020 ;

**VISTI** gli esiti delle verifiche effettuate in sede di collegio del 30 giugno 2022 Del n. 147;

**CONSIDERATO** che il potenziamento della rete cablata, in attuazione del progetto FESR-PON di cui all'Avviso Pubblico n. 20480 del 14.09.2021, ha apportato vantaggi in termini di protezione e sicurezza;

**RAVVISATA** la necessità di apportare conseguenti modifiche e aggiornamenti nei tempi di implementazione delle "*Misure minime di sicurezza ICT"* adottate;

VISTO il decreto dirigenziale n. 49 prot. n.0002199 del 16.03.2023 recante " *Misure minime di sicurezza ICT per le Pubbliche Amministrazioni. Pubblicazione del Modulo di Implementazione di cui all' Allegato 2 della Circolare AgID 2/2017" AGGIORNAMENTO NEI TEMPI DI IMPLEMENTAZIONE*

**RIAGGIORNA E ADOTTA**

le seguenti misure minime di sicurezza ICT per le Pubbliche Amministrazioni, descritte nell'allegato Modulo di Implementazione, al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informatici, ai sensi dell'art. 3 del D.Lgs 82/2015.

## Struttura e architettura della rete

In seguito all'attuazione del progetto FESR-PON di cui all'Avviso Publico n. 20480 del 14.09.2021, si è provveduto a riorganizzare e potenziare le reti WiFi esistenti nei tre plessi dell'Istituto, per assicurare una copertura ottimale, e prestazioni accettabili per tipologia e velocità, mediante la configurazione iniziale degli apparati passivi con fibra ottica a 10 GB e cavi di connessione UTP cat.6 e attivi,( access point professionali dual radio e dorsali in fibra ottica per velocità fino a 10 Gigabit) con la separazione tramite VLAN della segreteria dalla didattica, con reti wireless distinte tra docenti ed allievi, e politiche differenziate nel firewall per ogni tipologia di utente.

Attualmente l'Istituto dispone di :

una rete con collegamento fisico con Ethernet o con Hot-spot e antenne Wi-Fi:

- **una rete per la didattica** con collegamento fisico con Ethernet o con Hot-spot e antenne Wi-Fi all'interno dei laboratori e delle aule) per l'uso del registro elettronico e delle attività connesse all'uso dei "monitor digitali" e delle LIM.

- **una rete per gli Uffici di Segreteria** con collegamento fisico con Ethernet o con Hot-spot e antenne Wi-Fi, condivisa in modalità client server per applicativi quali, rilevazione presenze, gestione personale, magazzino… e gestita in cloud attraverso software proprietario Axios per la gestione del Protocollo, degli Alunni e del Registro Elettronico.

## Valutazione del rischio, misure di prevenzione

Il rischio dell' attuale rete dell' Istituto è di livello basso. Con gli interventi legati al progetto 13.1.1A-FESRPON-PU-2021-506 "Cablaggio strutturato e sicuro all'interno degli edifici scolastici" autorizzato con nota M.I. prot. AOODGEFID – 0040055 del 14.10. 2021, si è provveduto oltre che a potenziare l'intera rete, a installare in tutti i plessi un FIREWALL HARDWARE AVANZATO con throughput firewall 11500 Mbit/s, throughput con filtro applicazioni e deep packet inspection del traffico criptato attivo che monitora, traccia e controlla i dati in entrata e in uscita e il traffico di rete e assicura una protezione contro le minacce web tipo malware.

Il Dirigente Scolastico è supportato dal Responsabile della transizione digitale, dal Responsabile tecnico, dal Direttore SGA e dagli operatori di segreteria.

Le misure aggiornate vengono descritte nell'Allegato n.1: ***Modulo implementazione - Misure minime.***

**IL DIRIGENTE SCOLASTICO**

**Francesca CHIECHI**

**IL RESPONSABILE DELLA TRANSIZIONE DIGITALE**

**Gennaro CAMPOREALE**

- **A tutto il Personale**
- **All'Albo on-line**
- **Amministrazione Trasparente (sez. Disposizioni generali - Atti amministrativi generali)**
- **Atti**

**SEDE**

## LEGENDA

### 1. Acronimi utilizzati nella circolare AGID n. 2 del 18/04/2017 e inseriti nel modulo di implementazione di cui all'Allegato n.1.

| 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. |

### 2. Livelli di sicurezza indicati.

Nel documento, per ogni singola implementazione tecnica, è indicato il relativo livello di sicurezza.

| Sigla | Significato | Note |
|---|---|---|
| M | MINIMO | **Livello sotto il quale nessuna amministrazione può scendere**. Le misure previste dal livello minimo devono essere **messe in atto quanto prima**, poiché ritenute **necessarie** dall'AgID. I controlli indicati debbono riguardarsi come **obbligatori.** |
| S | STANDARD | Le misure previste dal livello STANDARD, rappresentano la **Base di riferimento per un livello di sicurezza completo**: il primo step e secondo sterp a cui tendere per la protezione della propria infrastruttura informatica. |
| A | ALTO | Le misure previste dal livello ALTO, rappresentano **l' Obiettivo finale a cui tendere**, per il completamento del piano di sicurezza. |

## 3. Tempi di implementazione

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

| | | | |
|---|---|---|---|
| 1. | Obiettivo strettamente necessario e quindi da attivare immediatamente per un livello di sicurezza necessario | primo step | Colore rosa |
| 2. | Obiettivo a cui tendere per un livello di sicurezza soddisfacente | secondo step | Colore azzurro |
| 3 | Obiettivo da prendere in considerazione per un livello di sicurezza completo | terzo step | Colore verde |
| 4 | Obiettivo finale da perseguire per raggiungere un livello di sicurezza ottimale | quarto step | Colore bianco |

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

Il presente documento contiene le informazioni riguardanti i sistemi in uso presso l'I.C. "Tommasone-Alighieri" di Lucera (Fg) per la gestione informatica, comprese le dei software AXIOS.

**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 | La scuola si è posta come obiettivo la messa in opera di tale implementazione.<br>Si prevede di predisporre un documento denominato" Inventario Hardware e Software firmato digitalmente.<br>L'inventario elencherà:<br>**a)**i dispositivi informatici collegati in rete **in modo permanente** o provvisorio e sarà strutturato nel modo seguente:<br>• **codice identificativo assegnato all'apparato (inventario patrimoniale);**<br>• **descrizione breve del tipo di dispositivo;**<br>• **MAC Address;**<br>• **indirizzo IP** (se statico; se invece l'indirizzo IP viene assegnato dinamicamente, verrà attiva la conservazione del log del DHCP server - vedi punti 1.2.1 e 1.2.2);<br>• **Collocazione e persona alla quale è assegnato**. |
| 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. | L'elenco di cui alla misura 1.1.1 è aggiornato.<br>L'aggiornamento dell'elenco è a carico dell' amministratore di sistema, nella fattispecie il dirigente scolastico, che si avvarrà della collaborazione di un suo delegato. |

| | | | | | |
|---|---|---|---|---|---|
| 1 | 3 | 2 | S | Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete. | La scuola si è posta come obiettivo la messa in opera di tale implementazione , |
| 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. | La scuola si è posta come obiettivo la messa in opera di tale implementazione<br>Vedi punto 1.1.1. |
| 1 | 4 | 2 | S | Per tutti i dispositivi che possiedono un indirizzo IP l'inventario deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale. | Vedi punto 1.1.1 |
| 1 | 4 | 3 | A | Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione. | Tutti gli accessi alla WLAN vengo eseguiti attraverso una whitelist dei dispositivi autorizzati. |
| 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. | La scuola si è posta come obiettivo la messa in opera di tale implementazione |
| 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. | La scuola si è posta come obiettivo la messa in opera di tale implementazione.<br><br>L'elenco è riportato in un documento (Inventario Hardware e Software.xlsx [scheda Software]) che è conservato presso l'ufficio del dirigente in apposita cartella che contiene tutti i documenti della scuola. L'inventario contiene:<br>• tipologia dispositivo<br>• nome del software<br>• fornitore e/o marca<br>• versione<br>• soggetto autorizzante<br>• eventuale data di scadenza dell'autorizzazione<br>L'aggiornamento dell'elenco dei software è a carico dei responsabili di laboratorio e del DSGA per la segreteria.<br>Sarano date direttive al personale e ai responsabili di non installare alcun software diverso.<br>In caso di necessità, questa verrà evidenziata ai responsabili che, dopo averne verificato la reale necessità, lo comunicheranno al Responsabile della Transizione digitale e all' Amministratore di Sistema (D.S.), ed eventualmente provvederanno affinché sia installato, come pure che venga aggiornato l'elenco. |
| 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. | La scuola si è posta come obiettivo la messa in opera di tale implementazione |
| 2 | 3 | 1 | M | Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato. | i responsabili di laboratorio eseguiranno periodicamente la verifica del software installato su ciascun dispositivo e compareranno il risultato con l'elenco di cui al punto 2.1.1.<br>Eventuale software installato che non risulti nell'elenco verrà segnalato all'Amministratore di Sistema, Responsabile della Transizione digitale che provvede affinché venga rimosso o, se valutato necessario, a che venga inserito nell'elenco. |
| 2 | 3 | 2 | S | Mantenere un inventario del software in tutta l'organizzazione che copra tutti i tipi di sistemi operativi in uso, compresi server, workstation e laptop. | |
| 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. | La scuola si è posta come obiettivo la messa in opera di tale implementazione. |
| 2 | 4 | 1 | A | Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete. | |

**ABSC 3 (CSC 3): PROTEGGERE LE CONFIGURAZIONI DI HARDWARE E SOFTWARE SUI DISPOSITIVI MOBILI, LAPTOP, WORKSTATION E SERVER**

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 3 | 1 | 1 | M | Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi. | Le configurazioni standard sono quelle già previste dai Sistemi Operativi che si ritengono sufficienti a garantire un livello di sicurezza adeguato per la rete didattica.<br><br>Per la rete di segreteria si prevede un antivirus per la navigazione in rete.<br>Tutte le macchine sono protette da password e hanno un antivirus installato. Gli utenti non hanno privilegi di amministratore. |
| 3 | 1 | 2 | S | Le configurazioni sicure standard devono corrispondere alle versioni "hardened" del sistema operativo e delle applicazioni installate. La procedura di hardening comprende tipicamente: eliminazione degli account non necessari (compresi gli account di servizio), disattivazione o eliminazione dei servizi non necessari, configurazione di stack e heaps non eseguibili, applicazione di patch, chiusura di porte di rete aperte e non utilizzate. | |
| 3 | 1 | 3 | A | Assicurare con regolarità la validazione e l'aggiornamento delle immagini d'installazione nella loro configurazione di sicurezza anche in considerazione delle più recenti vulnerabilità e vettori di attacco. | |
| 3 | 2 | 1 | M | Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione. | Le configurazioni standard sono quelle già previste dai Sistemi Operativi che si ritengono sufficienti a garantire un livello di sicurezza adeguato per la rete didattica.<br>Per la rete di segreteria si prevede un antivirus per la navigazione in rete.<br>Come da punto 3.1.1 |
| 3 | 2 | 2 | M | Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard. | Sono state date disposizioni in tal senso al responsabile tecnico esterno. Si procederà quindi ad eseguire il punto di ripristino del sistema più recente e ad aggiornare il sistema operativo di tutti i dispositivi |
| 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. | La scuola si è posta come obiettivo la messa in opera di tale implementazione<br>Per i laboratori didattici, non si ritiene necessario attivare immagini di ripristino; poiché per i laboratori didattici non esistono dati da preservare nel tempo e anche perché il ripristino puo' avvenire mediante clonazione di altri HD o mediante un ripristino totale del sistema.<br>Per gli uffici si ritiene necessario attivare immagini di ripristino iniziale ed effettuare soprattutto backup ricorrenti a cadenza prestabilite di dati ed altri software in locale. |
| 3 | 3 | 2 | S | Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati. | La scuola si è posta come obiettivo la messa in opera di tale implementazione |
| 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). | Attualmente la rete didattica e la rete di segreteria costituiscono un unico segmento con<br>collegamento fisico con Ethernet o con Hot-spot e antenne Wi-Fi.<br>La scuola si è posta come obiettivo la messa in opera di tale implementazione mediante la separazione delle due reti. |
| 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. | La scuola si è posta come obiettivo la messa in opera di tale implementazione mediante la separazione delle due reti. |
| 3 | 5 | 2 | A | Nel caso in cui la verifica di cui al punto precedente venga eseguita da uno strumento automatico, per qualunque alterazione di tali file deve essere generato un alert. | |
| 3 | 5 | 3 | A | Per il supporto alle analisi, il sistema di segnalazione deve essere in grado di mostrare la cronologia dei cambiamenti della configurazione nel tempo e identificare chi ha eseguito ciascuna modifica. | |
| 3 | 5 | 4 | A | I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle. | |
| 3 | 6 | 1 | A | Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate. | |

| | | | | | |
|---|---|---|---|---|---|
| 3 | 7 | 1 | A | Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard. | La scuola si è posta come obiettivo la messa in opera di tale implementazione mediante la separazione delle due reti. |

**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. | Per la segreteria si utilizza il software antivirus.<br>Si prevede in aggiunta l'acquisto del software di scansione vulnerabilità.<br>Per la didattica non sono necessari software specifici.<br>I responsabili di laboratorio sono informati sulla necessità di monitorare tutti i sistemi in rete, a fronte di una significativa modifica (installazione di un sistema o software nuovo, aggiornamento, modifica della configurazione) di uno o più sistemi o software come indicato nel punto 2.3.1. |
| 4 | 1 | 2 | S | Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura. | La scuola si è posta come obiettivo la messa in opera di tale implementazione mediante la separazione delle due reti. |
| 4 | 1 | 3 | A | Usare uno SCAP (Security Content Automation Protocol) di validazione della vulnerabilità che rilevi sia le vulnerabilità basate sul codice (come quelle descritte dalle voci Common Vulnerabilities ed Exposures) che quelle basate sulla configurazione (come elencate nel Common Configuration Enumeration Project). | |
| 4 | 2 | 1 | S | Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità. | |
| 4 | 2 | 2 | S | Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità | |
| 4 | 2 | 3 | S | Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile. | |
| 4 | 3 | 1 | S | Eseguire le scansioni di vulnerabilità in modalità privilegiata, sia localmente, sia da remoto, utilizzando un account dedicato che non deve essere usato per nessun'altra attività di amministrazione. | La scuola si è posta come obiettivo la messa in opera di tale implementazione mediante la separazione delle due reti. |

| | | | | | |
|---|---|---|---|---|---|
| 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. | La scuola si è posta come obiettivo la messa in opera di tale implementazione mediante la separazione delle due reti. |
| 4 | 4 | 1 | M | Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza. | La scuola si è posta come obiettivo la messa in opera di tale implementazione mediante la separazione delle due reti e con l'installazione di antivirus configurati per l'aggiornamento automatico |
| 4 | 4 | 2 | S | Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione | La scuola si è posta come obiettivo la messa in opera di tale implementazione mediante la separazione delle due reti. |
| 4 | 5 | 1 | M | Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni. | Gli aggiornamenti automatici sono abilitati su tutti i sistemi operativi non dismessi dalla microsoft. Si dà incarico al responsabile tecnico di aggiornare i sistemi operativi dei dispositivi per usufruire degli aggiornamenti automatici. |
| 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. | |
| 4 | 6 | 1 | S | Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite. | |
| 4 | 7 | 1 | M | Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando opportune contromisure oppure documentando e accettando un ragionevole rischio. | La scuola si è posta come obiettivo la messa in opera di tale implementazione |
| 4 | 7 | 2 | S | Rivedere periodicamente l'accettazione dei rischi di vulnerabilità esistenti per determinare se misure più recenti o successive patch possono essere risolutive o se le condizioni sono cambiate, con la conseguente modifica del livello di rischio. | |
| 4 | 8 | 1 | M | Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità , del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.). | Verrà redatto il DPP (Documento Programmatico in materia di Privacy) per la gestione del trattamento dati e del rischio informatico in generale. |

| | | | | | |
|---|---|---|---|---|---|
| 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. | |
| 4 | 9 | 1 | S | Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione. | |
| 4 | 10 | 1 | S | Valutare in un opportuno ambiente di test le patch dei prodotti non standard (es.: quelli sviluppati ad hoc) prima di installarle nei sistemi in esercizio. | |

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

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 5 | 1 | 1 | M | Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi. | Agli operatori di segreteria sono state impartite adeguate istruzioni in merito<br>La scuola ha sottoscritto un contratto con 1 tecnico specializzato per le attività di amministrazione. |
| 5 | 1 | 2 | M | Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato. | Non è necessario registrare gli accessi nella rete di segreteria poiché vi è un rapporto 1:1 tra operatore e dispositivo.<br>La rete didattica non presenta tale necessità |
| 5 | 1 | 3 | S | Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa. | I prodotti Axios consentono, per ogni utente ed ogni funzionalità di indicare la tipologia di accesso possibile (CRUD)<br>Gli accessi ai server e ai servizi di gestione degli stessi sono monitorati. |
| 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 effettuate 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 Colud 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 verifcare 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 dell'untente |
| 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. | |
| 5 | 4 | 2 | S | Generare un'allerta quando viene aggiunta un'utenza amministrativa. | |
| 5 | 4 | 3 | S | Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa. | |
| 5 | 5 | 1 | S | Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa. | |
| 5 | 6 | 1 | A | Utilizzare sistemi di autenticazione a più fattori per tutti gli accessi amministrativi, inclusi gli accessi di amministrazione di dominio. L'autenticazione a più fattori può utilizzare diverse tecnologie, quali smart card, certificati digitali, one time password (OTP), token, biometria ed altri analoghi sistemi. | Axios consente di definire una serie di parametri che possono rendere<br>sicure le credenziali di accesso ai propri programmi fornite:<br>1. Verifica o meno del doppio accesso<br>2. Inserimento data generale di scadenza password<br>3. Numero di gg massimi per la validità del codice di accesso<br>4. Numero massimo diggda ultimo accesso per consentire ancora<br><br>stesso<br>5. Lunghezza minima del codice di accesso (in questo caso 14)<br>6. Numero minimo dei caratteri minuscoli<br>7. Numero minimo dei caratteri maiuscoli<br>8. Numero minimo dei caratteri numerici<br>9. Numero minimo dei caratter i speciali<br>In Axios Cloud verranno a breve implementate le stesse funzioni |

| | | | | | |
|---|---|---|---|---|---|
| 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). | Per l'accesso individuale al sito non è necessario impostare "password forte", in quanto ogni singolo puo' in qualsiasi momento modificare la propria password |
| 5 | 7 | 2 | S | Impedire che per le utenze amministrative vengano utilizzate credenziali deboli. | I parametri definiti in Axios 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). | Alcuni software obbligano il cambio password con cadenza prestabilita; in alternativa il cambio verrà eseguito periodicamente dagli operatori. |
| 5 | 7 | 4 | M | Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history). | Alcuni software sono configurati per impedire il riutilizzo delle ultime 6 password per tutti gli utenti, altrimenti sarà cura degli operatori evitare il riutilizzo di password precedenti. |
| 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. | Agli operatori di segreteria sono state impartite adeguate istruzioni al riguardo. |
| 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 gestisce lo storico password impedendo di fatto che possa essereriutilizzato un codice di accesso già utilizzato in precedenza.<br>In Axios Cloud sarà a breve implementata le medesima funzione. |
| 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 tipologiedi accesso per ogni utente/fun2ione (S.1,1M)<br>I server sono configurati in modo da Assicurare la completa |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse. |
| 5 | 10 | 2 | M | Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona. | Le utenze di segreteria sono assegnate alla singola persona. |
| 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. | Le credenziali sono disponibili solo per il personale autorizzato: (tecnico, DSGA e un assistente amministrativo). |
| 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. | Come previsto dal D.Lgs. 196/2003 Privacy,le credenziali saranno raccolte in busta chiusa e conservate dal responsabile del trattamento.<br>Le credenziali di accesso sono personali e quindi non possono essere conosciute da altri utenti .<br>Per quanto concerne i prodotti Axios tali credenziali sono gestite all'interno della base dati, l'accesso alla stessaèconsentito solo tramite i programmi Axios equindi secondo le regole di sicurezza enunciate. |
| 5 | 11 | 2 | M | Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette. | |

**ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE**

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 8 | 1 | 1 | M | Installare su tutti i sistemi connessi alla rete locale strumenti atti a rilevare la presenza e bloccare l'esecuzione di malware (antivirus locali). Tali strumenti sono mantenuti aggiornati in modo automatico. | Con il potenziamento della rete cablata in tutti i plessi è stato installato un FIREWALL HARDWARE AVANZATO con throughput firewall 11500 Mbit/s, throughput con filtro applicazioni e deep packet inspection del traffico criptato attivo che monitora, traccia e controlla i dati in entrata e in uscita e il traffico di rete e assicura una protezione contro le minacce web tipo malware. |
| 8 | 1 | 2 | M | Installare su tutti i dispositivi firewall ed IPS personali. | Su tutti i PC, portatili e server Windows attivare il firewall di Windows. |
| 8 | 1 | 3 | S | Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati. | |
| 8 | 2 | 1 | S | Tutti gli strumenti di cui in ABSC_8.1 sono monitorati e gestiti centralmente. Non è consentito agli utenti alterarne la configurazione. | |
| 8 | 2 | 2 | S | È possibile forzare manualmente dalla console centrale l'aggiornamento dei sistemi anti-malware installati su ciascun dispositivo. La corretta esecuzione dell'aggiornamento è automaticamente verificata e riportata alla console centrale. | |
| 8 | 2 | 3 | A | L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud. | |
| 8 | 3 | 1 | M | Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali. | Limitare l'uso di dispositivi esterni a quelli necessari per le attività di segreteria e di gestione REAxios per i docenti.<br>Ciò non è possibile per la rete didattica che per sua natura non può essere limitata ma deve essere estesa anche ai dispositivi personali degli alunni |
| 8 | 3 | 2 | A | Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni. | |
| 8 | 4 | 1 | S | Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base. | |
| 8 | 4 | 2 | A | Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | produttori di sistemi operativi. | |
| 8 | 5 | 1 | S | Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host. | Con il potenziamento della rete cablata il filtraggio è assicurato. |
| 8 | 5 | 2 | A | Installare sistemi di analisi avanzata del software sospetto. | La scuola si è posta come obiettivo la messa in opera di tale implementazione. |
| 8 | 6 | 1 | S | Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione. | |
| 8 | 7 | 1 | M | Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili. | Il firewall dei sistemi operativi blocca l'esecuzione automatica dei contenuti in quanto attivo su ogni sistema con livello sufficientemente alto. |
| 8 | 7 | 2 | M | Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file. | La scuola si è posta come obiettivo la messa in opera di tale implementazione. |
| 8 | 7 | 3 | M | Disattivare l'apertura automatica dei messaggi di posta elettronica. | I software di gestione della posta offrono tale funzionalità. |
| 8 | 7 | 4 | M | Disattivare l'anteprima automatica dei contenuti dei file. | Ogni dispositivo èdotato di software cheoffre tale funzionaltà . |
| 8 | 8 | 1 | M | Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione. | Ogni antivirus èconfiguratoper soddisfare questi criteri di i sicurezza. |
| 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. | Isoftware di gestione della posta offrono tale funzionalità. |
| 8 | 9 | 2 | M | Filtrare il contenuto del traffico web. | L'antivirus include funzioni di filtraggio e sono state date disposizioni agli operatori di configurare il software antivirus delle postazioni di lavoro in tal senso. |
| 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'antivirus include funzioni di filtraggio e sono state date disposizioni agli operatori di configurare il software antivirus delle postazioni di lavoro in tal senso. |
| 8 | 10 | 1 | S | Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento. | |
| 8 | 11 | 1 | S | Implementare una procedura di risposta agli incidenti che preveda la trasmissione al provider di sicurezza dei campioni di software sospetto per la generazione di firme personalizzate. | |

**ABSC 10 (CSC 10): COPIE DI SICUREZZA**

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 10 | 1 | 1 | M | Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema. | Il 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 dì cellulare, di un messaggio sull'esito dell'esecuzione delle copie.<br>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.<br>Axios Cloud effettua Backup del logo delle transazioni ogni 30 minuti Backup completo ogni giorno alle 2.00 clrca Retention dei backup 8/10 gg.<br>La scuola tramite staorage di rete, su cloud, e dispositivi di archiviazione effettua periodicamente copie di sicurezza almeno delle informazioni strettamente necessarie. |
| 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. 8.0.2.449S) |
| 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. |
| 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 copìe. 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.<br>Questo consente di rimanere a norma anche con l'utilizzo di Backup Cloud di Axios.<br>Axios Cloud consente l'accesso ai dati solo ai legittimi proprietari degli stessi. Tutte le transizioni Axios Cloud sono cifrate e protette da protocollo HTTPS. |

| | | | | | |
|---|---|---|---|---|---|
| 10 | 4 | 1 | M | Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza. | E' possibile effettuare una copia su un disco esterno, ad esempio, e poi isolare quest'ultimo dal sistema semplicemente scollegando il cavo dal server.<br>I backup Axios Cloud sono conformi a tutte le regole attuali per il Disaster Recovery. |

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

| ABSC_ID | | | Livello | Descrizione | Modalità di implementazione |
|---|---|---|---|---|---|
| 13 | 1 | 1 | M | Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza (dati rilevanti) e segnatamente quelli ai quali va applicata la protezione crittografica. | L'analisi dei livelli particolari di riservatezza sarà implementata attraverso la compartimentazione dei dati in cartelle il cui accesso sarà fisicamente controllato e protetto da password. |
| 13 | 2 | 1 | S | Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti. | L'analisi dei livelli particolari di riservatezza sarà implementata attraverso la compartimentazione dei dati in cartelle il cui accesso sarà fisicamente controllato e protetto da password. |
| 13 | 3 | 1 | A | Utilizzare sul perimetro della rete strumenti automatici per bloccare, limitare ovvero monitorare in maniera puntuale, sul traffico uscente dalla propria rete, l'impiego di crittografia non autorizzata o l'accesso a siti che consentano lo scambio e la potenziale esfiltrazione di informazioni. | |
| 13 | 4 | 1 | A | Effettuare periodiche scansioni, attraverso sistemi automatizzati, in grado di rilevare sui server la presenza di specifici "data pattern", significativi per l'Amministrazione, al fine di evidenziare l'esistenza di dati rilevanti in chiaro. | |
| 13 | 5 | 1 | A | Nel caso in cui non sia strettamente necessario l'utilizzo di dispositivi esterni, implementare sistemi/configurazioni che impediscano la scrittura di dati su tali supporti. | |
| 13 | 5 | 2 | A | Utilizzare strumenti software centralizzati atti a gestire il collegamento alle workstation/server dei soli dispositivi esterni autorizzati (in base a numero seriale o altre proprietà univoche) cifrando i relativi dati. Mantenere una lista aggiornata di tali dispositivi. | |
| 13 | 6 | 1 | A | Implementare strumenti DLP (Data Loss Prevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie. | |
| 13 | 6 | 2 | A | Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line. | |
| 13 | 7 | 1 | A | Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto. | |
| 13 | 8 | 1 | M | Bloccare il traffico da e verso url presenti in una blacklist. | L'antivirus includerà funzioni di filtraggio; se necessario verranno aggiunti nella blacklist gli URL da bloccare. |

| | | | | | |
|---|---|---|---|---|---|
| 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. | |


**IL DIRIGENTE SCOLASTICO**

**Francesca CHIECHI**

Documento firmato digitalmente ai sensi del c.d.
Codice dell'Amministrazione Digitale e normativa connessa