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	**Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP** **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.** **Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.**
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	- Da implementare nell'a.s. 2018-19
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	- Da implementare nell'a.s. 2018-19
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	- Da implementare nell'a.s. 2018-19
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	- Da implementare nell'a.s. 2018-19
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	- Da implementare nell'a.s. 2018-19
1	3	1	**M**	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	- **Da implementare nell'a.s. 2017-18**
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	- Da implementare nell'a.s. 2017-18
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.	- **In fase di completamento**
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	- In fase di completamento

				titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	- Gestione con un CTRL Gateway
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.	- Gestione con un CTRL Gateway
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	- Gestione con un CTRL Gateway

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.	- **In fase di completamento**
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.	- Da implementare nell'a.s. 2017-18
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).	- Da implementare nell'a.s. 2017-18
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state	- Da implementare nell'a.s. 2017-18

				modificate.	
2	3	1	**M**	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	**Sistemi monitorati regolarmente dalle FFSS**
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.	- Sistemi monitorati regolarmente dalle FFSS
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.	- Da implementare nell'a.s. 2017-18
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.	- Da implementare nell'a.s. 2019-20

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.	**E' stato implementato un sistema di rete client-server con dominio Microsoft e server Windows 2012R2 che garantisce gli standard di sicurezza in cui le configurazioni dei sistemi operativi dei client sono bloccate tramite Criteri di gruppo. Tutti gli accessi sono memorizzati all'interno del server dove sono presenti log degli accessi. E' presente un sistema di aggiornamento e patching delle macchine mediante WSUS che è una componente di server windows 2012R2 che permette la gestione centralizzata e automatizzata degli update dei client. Le credenziali gestite mediante Active Directory sono tutte nominative con requisiti di complessità (minimo 8 caratteri, con almeno un numero e una lettera maiuscola o carattere speciale), scadenza a 90 giorni e**

					cronologia delle password. **I PC degli uffici sono tutti supportati da Microsoft e di tipo Professional. Non sono presenti macchine con Windows XP**
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.	- Da implementare nell'a.s. 2019-20
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.	- Da implementare nell'a.s. 2019-20
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	- **VEDI 3.1.1**
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	**Sono state date disposizioni agli addetti backup in tal senso.**
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	- Da implementare nell'a.s. 2019-20
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	**Tali immagini sono memorizzate e incluse nei backup periodici.**
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	- Da implementare nell'a.s. 2019-20
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).	**Tutte le operazioni di amministrazione remota sono effettuate per mezzo di connessioni protette utilizzando il software Teamviewer che utilizza durante le connessioni un metodo di crittografia basato sullo scambio di chiavi private/pubbliche 2048 RSA e un certificato AES a 256 bit**

					per la crittografia delle sessioni e il traffico rete.
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.	- Da implementare nell'a.s. 2019-20
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.	- Da implementare nell'a.s. 2019-20
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.	- Da implementare nell'a.s. 2019-20
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	- Da implementare nell'a.s. 2019-20
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	- Da implementare nell'a.s. 2019-20
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	- Da implementare nell'a.s. 2019-20

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 è presente il software antivirus Kaspersky Internet Security che esegue periodicamente oltre alla scansione antivirus una scansione delle vulnerabilità sulle macchine con relativi report inoltre ad ogni modifica della configurazione viene eseguito un controllo vulnerabilità dagli amministratori di sistema.** **Tale software si aggiorna automaticamente in regime di**

					validità di licenza.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	- Da implementare nell'a.s. 2019-20
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).	- Da implementare nell'a.s. 2019-20
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	- Da implementare nell'a.s. 2019-20
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	- Da implementare nell'a.s. 2019-20
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	- Da implementare nell'a.s. 2019-20
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.	- Da implementare nell'a.s. 2019-20
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.	- Da implementare nell'a.s. 2019-20
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	**Il software antivirus Kaspersky Internet Security è periodicamente aggiornato automaticamente.**
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	- Da implementare nell'a.s. 2019-20
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	**Per i sistemi operativi e le applicazioni Microsoft, è presente un sistema di aggiornamento e patching delle macchine mediante WSUS che è una componente di server windows 2012R2 che permette la gestione centralizzata e**

					automatizzata degli update dei client.
4	5	2	**M**	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	**Non risultano configurati sistemi air-gapped.**
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.	- Da implementare nell'a.s. 2019-20
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.	**Vedi 4.5.1** **In caso di vulnerabilità emerse di software per i quali non è gestito il patching automatico, gli amministratori di sistema si occupano di applicare le relative patch o di implementare opportune contromisure, altrimenti documentano il rischio che la scuola corre non accettando le contromisure da applicare.**
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.	- Da implementare nell'a.s. 2019-20
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.).	**Da implementare nell'a.s. 2019-20**
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.	**Sistemi monitorati regolarmente dalle FFSS**
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.	- Da implementare nell'a.s. 2019-20
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.	- Da implementare nell'a.s. 2019-20

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.	**Gli accessi alle risorse sono amministrati secondo il principio del privilegio minimo e della separazione delle funzioni L'accesso alle risorse e ai sistemi è limitato secondo il principio di minima funzionalità**
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	**Le utenze amministrative e direzionali utilizzano un canale diverso rispetto all'utilizzo per la didattica, ognuno dei due sistemi è dotato di firewall e sistemi di sicurezza propri Tutti gli accessi sono memorizzati all'interno del server essendo quasi tutte le macchine iscritte in un dominio microsoft che contiene tutti le utenze e relativi privilegi assegnati.**
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	- Sistemi monitorati e gestiti regolarmente da DS
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	**I documenti di nomina dei responsabili di laboratorio e degli assistenti amministrativi sono archiviati in segreteria.**
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	- Sistemi monitorati e gestiti regolarmente da DSGA
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.	**Agli operatori sono state impartite istruzioni al riguardo**
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	- Sistemi monitorati e gestiti regolarmente da DSGA
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	- Sistemi monitorati e gestiti regolarmente da DSGA
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di	- Sistemi monitorati e gestiti regolarmente da DSGA

				un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	- Sistemi monitorati e gestiti regolarmente da DSGA
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.	- Sistemi monitorati e gestiti regolarmente da DSGA
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).	- **VEDI 3.1.1**
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	- Sistemi monitorati e gestiti regolarmente da DSGA
5	7	3	**M**	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	- **VEDI 3.1.1**
5	7	4	**M**	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	- **VEDI 3.1.1**
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	- Sistemi monitorati e gestiti regolarmente da DSGA
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	- Sistemi monitorati e gestiti regolarmente da DSGA
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.	- Sistemi monitorati e gestiti regolarmente da DSGA
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.	- Sistemi monitorati e gestiti regolarmente da DSGA
5	10	1	**M**	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	**Sono definiti e resi noti ruoli e responsabilità inerenti la cybersecurity per tutto il personale e per eventuali terze parti rilevanti (es. fornitori, clienti, partner)**
5	10	2	**M**	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	**Ogni utente possiede una propria credenziale nominativa riconducibile alla singola persona con specifici privilegi**

					assegnati.
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.	**Agli operatori di segreteria e ai responsabili di laboratorio sono state fornite adeguate istruzioni a riguardo.**
5	10	4	S	Evitare l'uso di utenze amministrative locali per le macchine quando sono disponibili utenze amministrative di livello più elevato (e.g. dominio).	
5	11	1	**M**	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	**Le password vengono racchiuse in busta chiusa e conservate adeguatamente.**
5	11	2	**M**	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	**Le chiavi sono 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.	**Sistemi monitorati e gestiti regolarmente da DSGA, FFSS e DS** **PER SEGRETERIA VEDI 4.1.1 SU P.C. DEI LABORATORI E NOTEBOOK SONO PRESENTI ANTIVIRUS GRATUITI**
8	1	2	**M**	Installare su tutti i dispositivi firewall ed IPS personali.	**Tale funzionalità è presente nel software al punto 4.1.1**
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	- Sistemi monitorati e gestiti regolarmente da DS DSGA
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.	- Da implementare nell'a.s. 2019-20
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.	- Da implementare nell'a.s. 2019-20
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	- Da implementare nell'a.s. 2019-20

8	3	1	**M**	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	**Le attività di BYOD necessarie alla didattica utilizzano canali diversi di collegamento in rete e firewall rispetto a quello amministrativo e prevedono la registrazione automatica di nuovi dispositivi gestiti dall'amministratore** **È stata data disposizione al personale di segreteria di limitare l'uso di dispositivi esterni a quelli necessari per le attività di segreteria, ciò non è possibile per la rete didattica che per sua natura deve essere limitata ma talvolta può essere utilizzata anche dagli alunni, resta inteso che è comunque una rete fisicamente separata dalla rete di segreteria ed è protetta da password.**
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	- Da implementare nell'a.s. 2019-20
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.	- Da implementare nell'a.s. 2019-20
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	**E' presente un firewall Stormshield come componente di difesa perimetrale della rete uffici di segreteria, garantisce protezione in termini di sicurezza informatica mediante l'integrazione di tutte le principali funzioni di sicurezza (prevenzione contro le intrusioni IPS, firewalling applicativo e di rete, web-filtering, antivirus, antispam, QoS, monitoraggio del traffico nei tunnel VPN ed SSL, protezione del traffico VoIP ecc.). Esegue analisi del traffico e permette di bloccare il traffico da e verso url presenti in una blacklist. Sono state create delle regole e filtri per il traffico web. Viene effettuato il logging della navigazione.**
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.	- Da implementare nell'a.s. 2019-20
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	- Da implementare nell'a.s. 2019-20
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	- Da implementare nell'a.s. 2019-20

8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	**L'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili è disattivata.**
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	**L'esecuzione automatica dei contenuti dinamici presenti nei file è disattivata.**
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	**L'apertura automatica dei messaggi di posta elettronica è disattivata.**
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	**L'anteprima automatica dei contenuti dei file è disattivata.**
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	**All'inserimento dei supporti rimuovibili il software antivirus esegue una scansione automatica**
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.	**Il componente posta di Kaspersky Internet Security prevede anche un filtro della posta elettronica.**
8	9	2	M	Filtrare il contenuto del traffico web.	**Vedi 8.5.1**
8	9	3	M	Bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (e.g. .cab).	**Il fornitore dei servizi di posta (MIUR) si occupa di bloccare i messaggi con contenuti potenzialmente pericolosi. Inoltre Kaspersky Internet Security analizza il traffico web e di posta bloccando i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa**
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	- Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
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.	- Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate

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	**Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE**

				completo ripristino del sistema.	**Si procederà a breve all' acquisto e all' installazione e configurazione di un dispositivo NAS che permette di effettuare copie di sicurezza pianificate contenenti immagini del sistema operativo server, il desktop e i documenti degli utenti di segreteria, le share di rete e i database dei vari software gestionali che la scuola utilizza.**
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.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
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.	**Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE** **Il dispositivo NAS (vedi 10.1.1) verrà posizionato in in un luogo diverso rispetto al server e custodito e verrà utilizzato un sistema di cifratura per il backup dei dati.**
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.	**Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE** **Saranno implementate politiche di funzionamento del NAS che ne impediscono l'accesso in maniera permanente**

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	**Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE** **I dati con particolari requisiti di riservatezza sono stati identificati e a breve verranno applicate protezioni crittografiche.**
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per

				che contengono informazioni rilevanti	la AMMINISTRATIVA E DIREZIONALE
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.	**Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE** **VEDI 8.5.1**
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.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
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.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
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.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
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.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE
13	8	1	**M**	Bloccare il traffico da e verso url presenti in una blacklist.	**Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE** **VEDI 8.5.1.**
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.	- Sistemi monitorati e gestiti regolarmente da DS e DSGA per la AMMINISTRATIVA E DIREZIONALE