



## ISTITUTO COMPRESIVO STATALE "E. SPRINGER"

Scuola Infanzia- Scuola Primaria – Scuola secondaria di 1° grado

Scuola sec. 1° Surbo Tel. 0832.360890 Uff. Dirigente Tel. 0832.360891 Uff. Segreteria Tel. 0832.360892 Uff. D.S.G.A.

Scuola Prim. Giorgilorio Tel. 0832.360893 Scuola Inf. Giorgilorio Tel. 0832.360894

Via Toscanini 1 73010 SURBO(LE) - e-mail leic89900c@istruzione.it, e-mail certificata: leic89900c@pec.istruzione.it  
c.f. 80019410754 www.istitutocomprensivosurbo.gov.it

### MISURE MINIME DI SICUREZZA ICT

#### “MODULO DI IMPLEMENTAZIONE”

Visto il decreto legislativo 7 marzo 2005, n. 82 del C.A.D., che attribuisce all'AgID l'emanazione di regole, standard e guide tecniche, nonché di vigilanza e controllo sul rispetto delle norme di cui al medesimo C.A.D., anche attraverso l'adozione di atti amministrativi generali, in materia di sicurezza informatica;

Vista la direttiva del 1° agosto 2015 del Presidente del Consiglio dei ministri che impone l'adozione di standard minimi di prevenzione e reazione ad eventi cibernetici e che individua nell'Agenzia per l'Italia digitale l'organismo che dovrà rendere prontamente disponibili gli indicatori degli standard di riferimento, in linea con quelli posseduti dai maggiori partner del nostro Paese e dalle organizzazioni internazionali di cui l'Italia è parte;

Vista la Circolare AgID n. 2/2017 del 18.04.2017 che sostituisce la Circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni. (Direttiva del Presidente del Consiglio dei ministri 1° agosto 2015)» e che indica nell'allegato 1 tali misure;

Tenuto conto altresì della relativa circolare MIUR n. 3015 del 20 Dicembre 2017;

Viene elaborato il seguente “modulo di implementazione” relativo alle misure minime di sicurezza ICT da adottare in questo Istituto Scolastico.

#### 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	<ul style="list-style-type: none"><li>• Gestire l'inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l'indirizzo IP</li></ul>
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	<ul style="list-style-type: none"><li>• Da implementare nell'a.s. 2018-19</li></ul>

1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	<ul style="list-style-type: none"> <li>• Da implementare nell'a.s. 2018-19</li> </ul>
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	<ul style="list-style-type: none"> <li>• Da implementare nell'a.s. 2018-19</li> </ul>
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	<ul style="list-style-type: none"> <li>• Da implementare nell'a.s. 2018-19</li> </ul>
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	<ul style="list-style-type: none"> <li>• Da implementare nell'a.s. 2018-19</li> </ul>
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	<ul style="list-style-type: none"> <li>• Le macchine possono essere collegate solo previa registrazione di MAC e IP in inventario</li> </ul>
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	<ul style="list-style-type: none"> <li>• Le macchine possono essere collegate solo previa registrazione di MAC e IP in inventario</li> </ul>
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.	<ul style="list-style-type: none"> <li>• Da implementare entro fine a.s. 2017-18</li> </ul>
1	4	2	S	Per tutti i dispositivi che possiedono un indirizzo IP l'inventario	<ul style="list-style-type: none"> <li>• Da implementare nell'a.s. 2018-19</li> </ul>

				deve indicare i nomi delle macchine, la funzione del sistema, un titolare responsabile della risorsa e l'ufficio associato. L'inventario delle risorse creato deve inoltre includere informazioni sul fatto che il dispositivo sia portatile e/o personale.	
1	4	3	A	Dispositivi come telefoni cellulari, tablet, laptop e altri dispositivi elettronici portatili che memorizzano o elaborano dati devono essere identificati, a prescindere che siano collegati o meno alla rete dell'organizzazione.	Da implementare nell'a.s. 2019-20
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.	Da implementare nell'a.s. 2019-20
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.	L'installazione di software è bloccata per tutti gli utenti. Eventuali nuovi software sono installati esclusivamente dall'amministratore dopo verifica della tipologia e della funzionalità. Comunque un elenco dei software autorizzati è 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 entro fine 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 entro fine a.s. 2017-18
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per	Da implementare nell'a.s. 2019-20

				verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Una scansione a ritmi regolari è attuata per rilevare la presenza di software non autorizzati.
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.	Da implementare nell'a.s. 2019-20
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. 2019-20
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.	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.	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	Sistemi monitorati regolarmente dalle FFSS

				workstation, server e altri tipi di sistemi usati dall'organizzazione.	
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Sistemi monitorati regolarmente dalle FFSS
3	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Sistemi monitorati regolarmente dalle FFSS
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	4	1	M	Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).	Le operazioni di amministrazione da remoto sono impedito. In caso di necessità vengono abilitate temporaneamente connessioni attraverso protocolli sicuri e disabilitate al termine dell'intervento.
3	5	1	S	Utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema (compresi eseguibili di sistema e delle applicazioni sensibili, librerie e configurazioni) non siano stati alterati.	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.	Sistemi monitorati regolarmente dalle FFSS
4	1	2	S	Eeguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Da implementare nell'a.s. 2018-19
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. 2018-19
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Da implementare nell'a.s. 2018-19
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Da implementare nell'a.s. 2018-19
4	3	1	S	Eeguire 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. 2018-19
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. 2018-19
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Gli antivirus sono configurati per l'aggiornamento automatico
4	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole	Da implementare nell'a.s. 2018-19

				per aggiornare le attività di scansione	
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	I dispositivi sono configurati per l'aggiornamento automatico del SO
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Non vi sono sistemi separati dalla rete.
4	6	1	S	Verificare regolarmente che tutte le attività di scansione effettuate con gli account aventi privilegi di amministratore siano state eseguite secondo delle policy predefinite.	Da implementare nell'a.s. 2018-19
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.	Sistemi monitorati regolarmente dalle FFSS
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. 2018-19
4	8	1	M	Definire un piano di gestione dei rischi che tenga conto dei livelli di gravità delle vulnerabilità, del potenziale impatto e della tipologia degli apparati (e.g. server esposti, server interni, PdL, portatili, etc.).	Esistono procedure automatizzate di backup per la salvaguardia dei dati residenti in sede.
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Tutte le patch relative a vulnerabilità vengono immediatamente implementate appena disponibili
4	9	1	S	Prevedere, in caso di nuove vulnerabilità, misure alternative se non sono immediatamente disponibili patch o se i tempi di distribuzione non sono compatibili con quelli fissati dall'organizzazione.	Da implementare nell'a.s. 2018-19
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. 2018-19

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.	Sistemi monitorati e gestiti regolarmente da DS e DSGA e dall'animatore digitale dell'Istituto.
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
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Sistemi monitorati e gestiti regolarmente da DSGA
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Sistemi monitorati e gestiti regolarmente da DS e DSGA
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.	Sistemi monitorati e gestiti regolarmente da DSGA
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Da implementare nell'a.s. 2018-19
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Da implementare nell'a.s. 2018-19
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Da implementare nell'a.s. 2018-19
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Da implementare nell'a.s. 2018-19
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.	Da implementare nell'a.s. 2019-20



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).	Sistemi monitorati e gestiti regolarmente da DSGA. Le password devono includere lettere maiuscole e minuscole, caratteri speciali e numeri.
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Da implementare nell'a.s. 2018-19
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Sistemi monitorati e gestiti regolarmente da DSGA. Per le password viene imposta una scadenza trimestrale o semestrale in funzione del grado di criticità.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non è possibile riutilizzare password precedentemente utilizzate.
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Da implementare nell'a.s. 2018-19
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Da implementare nell'a.s. 2018-19
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.	Da implementare nell'a.s. 2018-19
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.	Da implementare nell'a.s. 2018-19
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	La distinzione è assicurata nella configurazione del server.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Sono associate a nome e cognome degli utenti ad ogni credenziale di accesso.
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.	Sistemi monitorati e gestiti regolarmente da DSGA
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).	Da implementare nell'a.s. 2018-19
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne	Sistemi monitorati e gestiti regolarmente da DSGA.

				disponibilità e riservatezza.	
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Sistemi monitorati e gestiti regolarmente da DSGA.

#### 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
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Sistemi monitorati e gestiti regolarmente da DSGA
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Da implementare nell'a.s. 2018-19
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. 2018-19
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. 2018-19
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.
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. 2018-19
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai	Da implementare nell'a.s. 2019-20

				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.	Da implementare nell'a.s. 2018-19
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. 2018-19
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimovibili al momento della loro connessione.	Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
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.	Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
8	9	2	M	Filtrare il contenuto del traffico web.	Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
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).	Sistemi monitorati e gestiti regolarmente da FFSS e regolamentate
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Da implementare nell'a.s. 2018-19
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.	Da implementare nell'a.s. 2018-19

#### 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	Il backup è effettuato automaticamente ogni giorno.

				almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	
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.	Da implementare nell'a.s. 2019-20
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Da implementare nell'a.s. 2019-20
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Da implementare nell'a.s. 2018-19
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 parte amministrativa e direzionale
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 parte amministrativa e direzionale

#### 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 parte amministrativa e direzionale
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Da implementare nell'a.s. 2018-19
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.	Da implementare nell'a.s. 2019-20
13	4	1	A	Effettuare periodiche scansioni, attraverso sistemi	Da implementare nell'a.s. 2019-20

				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.	Da implementare nell'a.s. 2019-20
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.	Da implementare nell'a.s. 2019-20
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.	Da implementare nell'a.s. 2019-20
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Da implementare nell'a.s. 2019-20
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Da implementare nell'a.s. 2019-20
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	La misura è implementata nel firewall
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	Da implementare nell'a.s. 2019-20

Surbo, 28 dicembre 2017

Il Dirigente scolastico

Prof.ssa Maria Rosaria manca