FONDI STRUTTURALI EUROPEI
UNIONE EUROPEA
PON 2014-2020
MIUR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l'istruzione e per l'innovazione digitale
Ufficio IV
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)

MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA

UFFICIO SCOLASTICO REGIONALE PER IL LAZIO

ISTITUTO DI ISTRUZIONE SUPERIORE "*BRAGAGLIA*"

Via Casale Ricci, s.n.c. – 03100 FROSINONE (FR)

Tel. 0775-291002 Fax 0775-202516 e-mail: fris01100q@istruzione.it e-mail pec: fris01100q@pec.istruzione.it

C.F.: 92057050608 C.M.: FRIS01100Q

- **LICEO ARTISTICO** "*A.G. Bragaglia* C. M. : FRSL011024
- **ISTITUTO PROFESSIONALE DI STATO PER L'INDUSTRIA E L'ARTIGIANATO** " *G. Galilei* "
  Corso Ordinario: C.M. FRRI01101B - Corso Serale: C.M. FRRI01151R - Sede Carceraria: C.M. FRRI01102C

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	E' stato dato incarico agli Amministratori di sistema di redigere un inventario che elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio.
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	E' stato dato incarico agli amministratori di sistema di redigere l'inventario e di curarne l'aggiornamento, di un inventario che elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

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.	E' stato dato incarico Agli Amministratori di sistema di redigere un elenco del software installato e le relative versioni. L'aggiornamento dell'elenco dei software è a carico degli Amministratori di Sistema. Sono state date direttive al personale ed agli amministratori di sistema di non installare alcun software diverso. In caso di necessità, questa viene evidenziata agli Amministratori di Sistema, che ne verificano la reale esigenza ed eventualmente provvedono affinché sia installato, come pure che venga aggiornato l'elenco. Le abilitazioni all'installazione del software sono stati concessi solamente agli amministratori di sistema (vedi 5.1.1)
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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).	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Gli Amministratori di Sistema eseguono periodicamente la verifica del software installato su ciascun dispositivo e comparano il risultato con l'elenco di cui al punto 2.1.1. Eventuale software installato che non risulti nell'elenco viene segnalato agli Amministratori di Sistema, che provvedono 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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

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.	Gli Amministratori di Sistema hanno definito e documentato le configurazioni sicure standard per ciascun sistema operativo utilizzato.
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,	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

				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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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 amministratori di sistema in tale senso.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Sono state date disposizioni agli amministratori di sistema di salvare le immagini d'installazione sul supporto Hard Disk di rete
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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).	I server remoti vengono amministrati da gestori esterni che provvedono alla sicurezza in modo autonomo.
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

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.	E' in corso l'adozione di una strumento informatico adeguato.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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).	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Sono state date disposizioni agli Amministratori di Sistema di verificare che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle vulnerabilità.
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	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Sono state date disposizioni agli Amministratori di Sistema di verificare che il software di scansione prima di ciascun utilizzo sia aggiornato rispetto alle vulnerabilità.
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.	Sono state date disposizioni agli Amministratori di Sistema di controllare ed aggiornare manualmente periodicamente i sistemi non raggiungibili via 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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	Sono state date disposizioni agli Amministratori di Sistema di verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie, gli Amministratori di Sistema documentano il caso, le eventuali contromisure o la motivazione della mancata risoluzioni su apposito registro/rapportino conservato presso l'Istituto

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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.).	Sono state date disposizioni agli amministratori di sistema di redigere il piano richiesto,
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.	Vedi 4.8.1 Sono state date disposizioni agli Amministratori di Sistema
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
5	1	1	M	Limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	I privilegi di amministratore sono riservati agli amministratori di sistema espressamente nominati da parte dell'ente. I privilegi di amministrazione per smartphone e tablet sono assegnati al soggetto al quale l'apparato è dato in dotazione dato che devono avere la possibilità di accettare in autonomia gli aggiornamenti di sicurezza.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	E' attivato il log di sistema per registrare gli accessi come amministratore su PC, server, apparati di rete.

5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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 degli amministratori di sistema sono consegnati agli stessi e una copia è conservata presso l'ufficio competente (vedi 5.11.1).
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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 amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

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).	Il sistema di autenticazione per tutti gli utenti obbliga all'utilizzo di password di autenticazioni "forti"
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Il sistema di autenticazione è configurato per obbligare tutti gli utenti al cambio password periodica.
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Il sistema di autenticazione è configurato per impedire il riutilizzo dell'ultima password per tutti gli utenti
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Agli amministratori di sistema sono state impartite adeguate istruzioni al riguardo.
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 amministratori di sistema sono state impartite adeguate istruzioni al 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).	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali amministrative non personali sono registrate su un apposito quaderno cartaceo conservato nella cassaforte della segreteria.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non si utilizzano certificati digitali per l'autenticazione delle utenze amministrative.

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.	Su tutti i PC, portatili e server è installato un antivirus con aggiornamento automatico.
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Su tutti i PC, portatili e server Windows è attivato il firewall di Windows. Sui server Linux è installato SHOREWALL
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Nel disciplinare dei dipendenti è stata data disposizione di limitare l'uso di dispositivi esterni a quelli necessari per le attività didattiche

8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	E' stata data disposizione agli amministratori di sistema di configurare in tal senso le postazioni di lavoro.
8	9	1	M	Filtrare il contenuto dei messaggi di posta prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.	L'Istituto utilizza un servizio di posta elettronica esterno, che include il filtraggio richiesto
8	9	2	M	Filtrare il contenuto del traffico web.	Sono state date disposizioni agli amministratori di sistema di attivare il filtraggio del contenuto sul traffico web.

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).	Sono state date disposizioni agli amministratori di sistema 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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

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.	E' implementato il sistema di ripristino in automatico di Windows
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	Sono state date disposizioni agli amministratori di sistema di configurare il software antivirus delle postazioni di lavoro in tal senso. Più specificatamente le copie di sicurezza sono conferite da parte di un operatore incaricato e conservate in un locale sicuro ad accesso controllato e in cassaforte.
10	4	1	M	Assicurarsi che i supporti contenenti almeno una delle copie non siano permanentemente accessibili dal sistema onde	E' stata data disposizione agli amministratori di sistema di configurare in tal senso il sistema di backup.

				evitare che attacchi su questo possano coinvolgere anche tutte le sue copie di sicurezza.	

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 è implementata attraverso la compartimentazione dei dati in cartelle il cui accesso è regolato da specifici criteri di accesso (ACL).
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
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.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Vedi misura 8.9.2
13	9	1	A	Assicurare che la copia di un file fatta in modo autorizzato mantenga le limitazioni di accesso della sorgente, ad esempio attraverso sistemi che implementino le regole di controllo degli accessi (e.g. Access Control List) anche quando i dati sono trasferiti al di fuori del loro repository.	*Misura non implementata in quanto ritenuta troppo complessa/onerosa rispetto alla relativa complessità del sistema informatico dell'Istituto*

Il Dirigente Scolastico

Prof. Fabio GIONA