ISTITUTO MAGISTRALE STATALE
"Regina Margherita"

Licei: Scienze Umane / Linguistico / Economico Sociale/ Musicale / Coreutico
P.tta SS. Salvatore, 1 - 90134 PALERMO
Codice Fiscale: 80019900820 - Cod. Min.: PAPM04000V – Cod. Univoco: UFCXJ5
Tel. 091.334424 / 334043 - Fax 091.6512106
E mail: papm04000v@istruzione.it – papm04000v@pec.istruzione.it
www.liceoreginamargherita.gov.it

Prot. N°. 16821/a35

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

Minimo; Standard; Avanzato

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	
1	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Installato software per la redazione automatica dell'Inventario delle risorse informatiche (server, personal computer, stampanti e apparati di rete)
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Effettuata la rilevazione degli apparati ed impostato il software di Inventory / Discovery per la segnalazione di allarmi in caso di anomalie
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Tramite auditing del traffico eseguita la qualificazione della tipologia dei sistemi collegati.
1	2	1	S	Implementare il "logging" delle operazione del server DHCP.	Implementato server DHCP sul server di dominio
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Implementate regole sul server di dominio per acquisire informazioni relative ai dispositivi collegati.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Eseguita configurazione del software di Audit / Inventory per la scansione automatica della rete, con l acquisizione delle nuove

					informazioni per i nuovi apparati collegati
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.	Inseriti manualmente nel file di excel relativo all 'inventario gli indirizzi ip degli apparati di rete collegati.
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.	I dispositivi appartenenti alla struttura amministrativa, vengono registrati come client di un DOMINIO (active directory) e sul server vengono registrate le informazioni relative all' utenza alla specificità del lavoro svolto. Inoltre il software di AUDIT provvede alla catalogazione dell'inventario hardware e software del dispositivo.
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.	I dispositivi "mobili "vengono registrati sulle politiche di sicurezza del firewall garantendo la tracciabilità e l'identificazione
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.	Configurato sistema WI-FI con accesso tramite password criptata. Implementato sul dispositivo firewall Hot Spot, con credenziali a tempo ed autenticazione tramite Mac address, Implementato sistema di controllo dei dispositivi collegati
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.	Implementata lista dei software non consentiti, eseguito controllo di tutti i pc e disinstallazione dei software non conformi.
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.	Eseguita configurazione dei client in dominio con utenze limitate, create delle regole per il blocco di software non conformi. Creata regole per l'utilizzo di software presente nella" whitelist" dei software consentiti
2	2	2	S	Per sistemi con funzioni specifiche (che richiedono solo un	Eseguita configurazione dei client in dominio con utenze limitate,

				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).	create delle regole per il blocco di software non conformi. Creata regole per l'utilizzo di software presente nella" whitelist" dei software consentiti. Utilizzata macchina virtuale per la configurazione di macchine specializzate
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Esecuzione periodica del comando per l'integrità dei file del sistema operativo
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Configurazione software per la rilevazione dei software installati
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.	Configurazione software per la rilevazione dei software installati
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.	Configurazione software per la rilevazione e per l'inventario dei software installati, completo dei dati relativi alla versione degli applicativi e delle versioni dei sistemi operativi. Eseguita configurazione automatica per la rilevazione del software non autorizzato
2	4	1	A	Utilizzare macchine virtuali e/o sistemi air-gapped per isolare ed eseguire applicazioni necessarie per operazioni strategiche o critiche dell'Ente, che a causa dell'elevato rischio non devono essere installate in ambienti direttamente collegati in rete.	

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
3	1	1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Eseguite installazioni standard dei client.
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,	Pulizia del sistema operativo dei vari client. Eliminati account non utilizzati e software non consentiti.

				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.	Eseguita la creazione d'immagini del disco, delle varie postazioni di lavoro
3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Create immagini iso dei dispositivi presenti nella struttura
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Creazione di immagini ISO, con installazioni standard per il pronto ripristino dei dispositivi danneggiati.
3	2	3	S	Le modifiche alla configurazione standard devono effettuate secondo le procedure di gestione dei cambiamenti.	Implementazione di regole client e server che non permettono l'installazione di applicativi diversi da quelli standard consentiti
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Memorizzazione delle ISO su dvd rom
3	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	I Backup delle immagini ISO vengono salvati su sistemi ad accesso esclusivo tramite l'utilizzo di credenziali e Chiavi di sicurezza
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).	Utilizzati software di controllo remoto protetto
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.	Impostate regole per scansioni
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.	Le regole creano automaticamente dei report
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.	Versionamento creando punti di ripristino
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Log delle modifiche e delle variazioni al sistema operativo

3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Regole client server per il monitoraggio di modifiche non autorizzate
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Configurato Software per amministratore di sistema

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.	Controllo delle funzionalità del sistema tramite software apposito.
4	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Gestione tramite software, degli applicativi installati e generazione dei report aggiornamenti Pianificazione delle scansioni di vulnerabilità
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).	Installato Software per il controllo delle vulnerabilità
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Verifica e catalogazione dei log su syslog server
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	Settato invio log vulnerabilità
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Impostato il software di amministrazione per la rilevazione e l allert degli attacchi nocivi
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	Configurazione di account dedicati alla sola scansione delle vulnerabilità

				amministrazione.	
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.	Gestione gruppi di scansione sul software amministrazione
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Impostati aggiornamenti automatici
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	Impostati aggiornamenti automatici distribuiti client server. Configurato Allert per le macchine da aggiornare Configurato software di amministrazione per ricevere allert e mail relative agli aggiornamenti sulle minacce e vulnerabilità
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Impostati aggiornamenti automatici
4	5	2	M	Assicurare l'aggiornamento dei sistemi separati dalla rete, in particolare di quelli air-gapped, adottando misure adeguate al loro livello di criticità.	Aggiornamenti stand-alone tramite Cd e Pendrive
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.	Individuate le patch correttive, configurato account per attivare le regole per la distribuzione degli aggiornamenti
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.	Impostati aggiornamenti automatici, verifica di funzionamento, redigere documento per la registrazione delle operazioni fatte ed eventuali rischi riscontrati.
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.	Configurato software di gestione di amministrazione per la rilevazione di modifiche e l'individuazione di rischi e allert. Relazione sulla analisi dei rischi
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.).	Relazione sui rischi e sulle minacce informatiche (pc che verificano la posta o sui quali si utilizzano pendrive)
4	8	2	M	Attribuire alle azioni per la risoluzione delle vulnerabilità un	Analisi dei rischi

				livello di priorità in base al rischio associato. In particolare applicare le patch per le vulnerabilità a partire da quelle più critiche.	Lista degli aggiornamenti critici ed installazioni degli stessi
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.	Verifica dei rischi
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.	Utilizzo di Macchine virtuali, per la verifica ed il controllo degli aggiornamenti

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.	Definite password locali di amministratore e consegnate solo ai responsabili.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Definite password utenze limitate per gli utenti standard Definite password di amministratore per gli amministratori Eseguita registrazione degli accessi per tipologia di utenza
5	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Create utenze nel controller di dominio account specializzati
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Salvataggio del registro eventi delle operazioni compiute
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Create buste utenze/ password, con la descrizione del livello di utenza,
5	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Creata unità insieme delle utenze di amministratore, creata regole per la registrazione delle variazioni delle utenze
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti	Cambio password di amministratore e creazione utenza locale

				con quelli delle utenze amministrative in uso.	
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Creare unità organizzativa contente le utenze disattivate
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Creata regola che genera un rapporto quando viene creato un utente amministratore (log del registro utenti e account)
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Creata regola che genera un rapporto quando viene modificato un utente a con privilegi superiori (log del registro utenti e account)
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Generato log degli accessi falliti
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.	
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).	Attivazione criteri di complessità delle password
5	7	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Attivazione criteri di complessità delle password sulle regole del dominio
5	7	3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Attivazione criteri di complessità delle password
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Attivazione criteri di complessità delle password
5	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Attivazione criteri di complessità delle password sulle regole del dominio
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Attivazione criteri di complessità delle password sulle regole del dominio
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.	Attivazione criteri di complessità delle password sulle regole del dominio
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.	Creata macchina virtuale ad esclusivo uso dell’amministratore della struttura

5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Creazione di utenze dedicate di amministratore locale e del dominio
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Completare le informazioni relative agli account
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.	Registrate in busta chiusa le utenze di “administrator” e “root”
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).	Utilizzo delle credenziali amministrative differenti dalle password di amministratore locali
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Registrate in busta chiusa le utenze di “administrator” come voluto dal DPS
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Backup dei ceritificati su dispositivi esterni (pendrive – cd-rom)

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.	Installazione di antivirus e attivazione aggiornamenti automatici
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Attivazione firewall locali e attivazione delle regole
8	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Installazione di antivirus client server e configurazione dei log.
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.	Installato antivirus client /server, con gestione centralizzata sul server
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	Installato antivirus client /server, con gestione centralizzata sul server

				automaticamente verificata e riportata alla console centrale.	
8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Utilizzo di macchina virtuale non connessa alla rete per l'esame e la verifica del funzionamento degli aggiornamenti
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Regole per il Blocco dei dispostivi esterni
8	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Regola che registra Log delle connessioni di dispositivi esterni
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	Utilizzo di software per il monitoraggio dalla struttura informatica e di rete. Installata macchina virtuale per il controllo delle vulnerabilità
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Eseguire Aggiornamenti dei 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.	Configurazione firewall sulla rete con controllo del traffico dati
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per il blocco di traffico e software sospetto Scansione real time dei software
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per il blocco del traffico
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Disattivata esecuzione automatica al momento dell'inserimento di dispositivi esterni (pendrive , cd-rom dvd-rom)
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Configurare sugli account le regole per il blocco delle macro
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Configurato il gestore della posta elettronica
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Configurato il gestore della posta elettronica
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Attivare scansione automatica dei dispositivi connessi
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.	Impostate regole antispam, sulle regole del firewall
8	9	2	M	Filtrare il contenuto del traffico web.	Attivato filtro contenuti sulle regole del firewall

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).	antispam Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per il blocco di traffico e software sospetto
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per il blocco di traffico e software sospetto Attivato software per il controllo anti-malware
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.	Impostato Antivirus per la segnalazione delle anomalie

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.	Pianificati backup settimanali
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.	Eseguita configurazione automatica dei backup su dispositivo NAS
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Eseguiti backup differenti su diversi dispositivi, collocati in luoghi fisicamente differenti.
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Programmazioni della verifica del “disaster recovery”
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.	Attivata cifratura dei Backup
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.	Eseguito backup su dispositivo hd esterno conservati in luoghi sicuri

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	Attivato backup con cifratura sui dati ritenuti sensibili
13	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	Attivati sistemi di cifratura e autenticazione per i dispositivi sensibili
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.	Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per il blocco di traffico e software sospetto
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.	Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per il blocco di traffico e software sospetto
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.	Attivate regole del dominio che consentono la scrittura su dispostivi esterni solamente agli utenti autorizzati
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.	Installato controller Wi-Fi per il controllo dei dispositivi mobili. Attivate regole sul dispositivo firewall per l'autorizzazione dei dispositivi connessi alla rete.
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.	Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per la rilevazione delle anomalie. Installato sul server software di controllo dei flussi di rete e esportazione dei report

13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per la rilevazione delle anomalie. Esportazione dei Log
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Configurazione firewall sulla rete con controllo del traffico dati e attivazione regole per la rilevazione delle anomalie.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Configurazione firewall sulla rete con attivazione filtro contenuti e blacklist.
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.	Attivato salvataggio con Crittografia con accesso esclusivo al proprietario del dato.

Responsabile gestione sito istituzionale – Prof.ssa Cascio Rosaria - Prot. n°. 16812/FP del 27/12/2017.

Responsabile per la trascrizione digitale ai sensi del D.Lgs. 82/05 – Sig. Corrao Giovanni - Prot. n°. 16813/FP del 27/12/2017.

IL DIRIGENTE SCOLASTICO

Prof.ssa Blandano Pia