ISTITUTO COMPRENSIVO POLO I

73013 GALATINA (LE) Piazza F. Cesari, 14

Tel: 0836566035 E-mail: leic887006@istruzione.it

Misure minime di sicurezza ICT

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

ABSC_ID	Livello	Descrizione	Stato	Modalità
1.1.1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	Implementata	Tutti i dispositivi attivi sono inventariati su un registro, tenuto a cura del responsabile della gestione privacy. Il registro è aggiornato ad ogni dismissione di dispositivo o di collegamento di nuovo dispositivo alla rete. Per ogni dispositivo vengono registrate almeno le seguenti informazioni: codice identificativo, nome del dispositivo, sistema operativo, indirizzo ip e tipologia.
1.1.2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	Non implementata	
1.1.3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	Non implementata	
1.1.4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	Non implementata	
1.2.1	S	Implementare il "logging" delle operazione del server DHCP.	Non implementata	
1.2.2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	Non implementata	
1.3.1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Implementata	v. ABSC_ID 1.1.1
1.3.2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	Non implementata	
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.	Implementata	v. ABSC_ID 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.	Non implementata	

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.	Non implementata	
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.	Non implementata	
1.6.1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	Non implementata	

ABSC 2 (CSC 2): INVENTARIO DEI SOFTWARE AUTORIZZATI E NON AUTORIZZATI

ABSC_ID	Livello	Descrizione	Stato	Modalità
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	Tutti i software autorizzati sono inventariati su un registro, tenuto a cura del responsabile della gestione privacy. Il registro è aggiornato periodicamente con cadenza almeno mensile, e comunque in occasione di aggiornamenti importanti delle versioni legate a rilasci di correttivi di vulnerabilità gravi. Per ogni software vengono registrate le seguenti informazioni: descrizione, categoria, produttore, versione, uso. Sono date adeguate istruzioni agli incaricati del trattamento affinché non installino autonomamente software non inclusi nell'elenco. Nel caso si renda necessario ai fini della produttività installare un nuovo software, questo deve essere autorizzato dal responsabile dei sistemi informatici.
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.	Non implementata	
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).	Non implementata	
2.2.3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	Non implementata	

2.3.1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Implementata	Periodicamente vengono eseguiti controlli, anche mediante strumenti automatici, sulle postazioni di lavoro da parte del responsabile dei sistemi informatici al fine di rilevare la presenza di software non autorizzati e potenzialmente rischiosi per la protezione dei dati e/o il funzionamento regolare dei programmi di produttività. Nel caso sia rilevata la presenza di software non autorizzati, il responsabile dei servizi informatici provvede all'immediata disinstallazione del software e a fare segnalazione al responsabile della gestione privacy dell'amministrazione.
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.	Non implementata	
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.	Non implementata	
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.	Non implementata	

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

ABSC_ID	Livello	Descrizione	Stato	Modalità
3.1.1	M	Utilizzare configurazioni sicure standard per la protezione dei sistemi operativi.	Implementata	La configurazione dei sistemi operativi viene effettuata dagli amministratori di sistema sulla base di impostazioni di sicurezza standard e delle finalità di utilizzo del dispositivo.
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.	Non implementata	
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.	Non implementata	

3.2.1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	Implementata	v. ABSC_ID 3.1.1
3.2.2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Implementata	Sono state fornite adeguate istruzioni al responsabile dei sistemi informatici affinché l'eventuale ripristino di dispositivi compromessi avvenga sempre mediante utilizzo di configurazioni standard sicure.
3.2.3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	Non implementata	
3.3.1	M	Le immagini d'installazione devono essere memorizzate offline.	Implementata	Le immagini di installazione/configurazione dei dispositivi vengono memorizzate su dispositivi non collegati alla rete e accessibili esclusivamente dal responsabilie dei servizi informartici e dal responsabile della gestione privacy dell'amministrazione.
3.3.2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	Non implementata	
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).	Implementata	Sono state fornite adeguate istruzioni ai manutentori della rete e agli amministratori di sistema affinché tutte le operazioni di amministrazione remota avvengano per mezzo di connessioni crittografate e protette come VPN e connessioni https.
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.	Non implementata	
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.	Non implementata	
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.	Non implementata	
3.5.4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	Non implementata	
3.6.1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	Non implementata	

3.7.1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	Non implementata	

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'

ABSC_ID	Livello	Descrizione	Stato	Modalità
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.	Implementata	Ad ogni aggiornamento significativo dei sistemi, gli amministratori di sistema mediante un apposito programma (vulnerability scanner) verificano la presenza di eventuali vulnerabilità (es. patch non eseguite), intervenendo prontamente in caso positivo per rimuoverle.
4.1.2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	Non implementata	
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).	Non implementata	
4.2.1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	Non implementata	
4.2.2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità.	Non implementata	
4.2.3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	Non implementata	
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.	Non implementata	
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.	Non implementata	
4.4.1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Implementata	Sono date istruzioni agli amministratori dei sistemi affinché provvedano a tenere sempre aggiornati i programmi utilizzati per la scansione delle 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.	Non implementata	
4.5.1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Implementata	Ogni dispositivo di lavoro viene configurato in modo da eseguire automaticamente la ricerca e l'installazione di nuovi aggiornamenti (Sistema Operativo e software installati).
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.	Implementata	Sono state date istruzioni agli amministratori dei sistemi affinché provvedano ad aggiornare anche eventuali sistemi non collegati alla 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.	Non implementata	
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.	Implementata	Al termine delle operazioni di correzione delle anomalie, gli amministratori di sistema addetti al controllo delle vulnerabilità procedono ad effettuare una nuova scansione al fine di verificare che le vulmerabilità rilevate siano state effettivamente risolte. Nel caso non sia possibile procedere alla risoluzione della vulnerabilità tramite patch, l'amministratore è tenuto a farne segnalazione al responsabile dei sistemi informatici e al responsabile della gestione privacy, i quali si attivano per adoperare contromisure adeguate per ricondurre il rischio entro limiti accettabili. Per le vulnerabilità critiche viene definito un piano di gestione rischi, in cui sono riportati i seguenti elementi: descrizione della vulnerabilità, impatto sui sistemi e sulla protezione dei dati personali, livello di rischio, azioni intraprese per ridurre il rischio. Ad ogni azione viene attribuito un livello di priorità.
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.	Non implementata	
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.).	Implementata	v. ABSC_ID 4.7.1
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.	Implementata	v. ABSC_ID 4.7.1

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.	Non implementata	
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.	Non implementata	

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

ABSC_ID	Livello	Descrizione	Stato	Modalità
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.	Implementata	L'attribuzione delle funzioni di amministratore è effettuata previa valutazione dell'esperienza, della capacità e dell'affidabilità del soggetto designato, conformemente a quanto stabilito dal Provvedimento del Garante della Privacy del 27 novembre 2008 e succ. modifiche, recante <<Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema>>.
5.1.2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Implementata	Conformemente a quanto stabilito dal Provvedimento del Garante della Privacy del 27 novembre 2008 e succ. modifiche, recante <<Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema>>, sono stati adottati sistemi di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Con cadenza almeno annuale viene svolto da parte del responsabile della gestione privacy una verifica dell'operato degli amministratori, mediante analisi degli access log.
5.1.3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	Non implementata	
5.1.4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	Non implementata	

5.2.1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	Implementata	Il registro degli amministratori di sistema, con l'elenco delle funzioni e delle utenze amministrative ad essi attribuite, è tenuto e viene aggiornato dal responsabile della gestione privacy, ad ogni variazione di ambito di operatività dell'incarico, di designazione di nuovo incarico o di fine rapporto. La designazione degli amministratori di sistema è individuale e reca l'elencazione analitica degli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato.
5.2.2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	Non implementata	
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.	Implementata	Sono state date istruzioni agli amministratori dei sistemi affinché, prima di collegare un nuovo dispositivo alla rete, ove possibile provvedano a reimpostare le credenziali di amministratore predefinito del dispositivo con valori coerenti con quelli delle utenze amministrative in uso.
5.4.1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	Non implementata	
5.4.2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	Non implementata	
5.4.3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	Non implementata	
5.5.1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	Non implementata	
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.	Non implementata	
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).	Implementata	Sono impostate adeguate regole di dominio affinché le password delle utenze amministrative siano assoggettate a vincoli in merito a: lunghezza, complessità, frequenza di modifica e cronologia.
5.7.2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	Non implementata	
5.7.3	M	Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging).	Implementata	v. ABSC_ID 5.7.1
5.7.4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Implementata	v. ABSC_ID 5.7.1

5.7.5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	Non implementata	
5.7.6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	Non implementata	
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.	Non implementata	
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.	Non implementata	
5.10.1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Implementata	Sono state fornite adeguate istruzioni agli amministratori di sistema affinché sia mantenuta una completa distinzione, attraverso uso di credenziali diverse, tra utenze privilegiate e non privilegiate degli operatori che svolgono anche incarichi in qualità di amministratore di sistema.
5.10.2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	Implementata	Sono state fornite adeguate istruzioni agli amministratori di sistema affinché tutte le utenze siano nominative e riconducibili ad una sola persona.
5.10.3	M	Le utenze amministrative anonime, quali "root" di UNIX o "Administrator" di Windows, debbono essere utilizzate solo per le situazioni di emergenza e le relative credenziali debbono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Implementata	Sono state fornite adeguate istruzioni agli amministratori di sistema affinché tutte le utenze amministrative anonime siano utilizzate solo per casi di emergenza. Il responsabile della gestione privacy esegue con cadenza almeno annuale controlli sugli access log, verificando la rispondenza dell'operato degli amministratori alle disposizioni ricevute.
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).	Non implementata	
5.11.1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Implementata	Sono state fornite adeguate istruzioni agli amministratori di sistema, e più in generale a tutti gli incaricati di trattamento che operano con strumenti informatici, affinché utilizzino la massima cautela nella conservazione e riservatezza delle loro credenziali di accesso. Le credenziali amministrative anonime, utilizzate per i casi di emergenza, sono conosciute oltre che dagli amministratori di sistema, anche dal responsabile della gestione privacy.
5.11.2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non Applicabile	Non viene fatto uso di certificati digitali per l'autenticazione degli amministratori di sistema.

ISTITUTO COMPRENSIVO POLO I

73013 GALATINA (LE) Piazza F. Cesari, 14

Tel: 0836566035 E-mail: leic887006@istruzione.it

ABSC 8 (CSC 8): DIFESE CONTRO I MALWARE

ABSC_ID	Livello	Descrizione	Stato	Modalità
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.	Implementata	In tutti i dispositivi collegati alla rete sono presenti e tenuti aggiornati in modalità automatica anti-malware.
8.1.2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Implementata	In tutti i dispositivi collegati alla rete sono presenti e tenuti aggiornati firewall e programmi anti intrusione.
8.1.3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	Non implementata	
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.	Non implementata	
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.	Non implementata	
8.2.3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	Non implementata	
8.3.1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali.	Implementata	Sono state date disposizioni agli amministratori di sistema e a tutti gli incaricati di trattamento che operano con strumenti informatici affinché limitino l'utilizzo di dispositivi esterni a casi di emergenza e solo se previamente autorizzati.
8.3.2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	Non implementata	
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.	Non implementata	
8.4.2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	Non implementata	
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.	Non implementata	
8.5.2	A	Installare sistemi di analisi avanzata del software sospetto.	Non implementata	
8.6.1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	Non implementata	

8.7.1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Implementata	Su tutte le postazioni di lavoro, è stata disattivata, da configurazione di sistema, l'esecuzione automatica di contenuti da dispositivi removibili.
8.7.2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Implementata	Sono state fornite adeguate disposizioni a tutti gli incaricati di trattamento che operano con strumenti informatici, affinché mantengano disattivata come impostazione di default l'esecuzione automatica dei contenuti dinamici presenti nei file.
8.7.3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	Implementata	Sono state fornite adeguate istruzioni a tutti gli incaricati di trattamento che operano con strumenti informatici affinché mantengano disattivata come impostazione di default l'apertura automatica delle email sui programmi di posta elettronica.
8.7.4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Implementata	Sono state fornite adeguate istruzioni a tutti gli incaricati di trattamento che operano con strumenti informatici affinché mantengano disattivata come impostazione di default l'anteprima automatica dei contenuti dei file.
8.8.1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Implementata	Su ciascuna postazione di lavoro si è provveduto a configurare l'antivirus in modo da eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.
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.	Implementata	Su ciascuna postazione di lavoro si è provveduto a configurare l'antivirus in modo da eseguire una scansione antivirus dei messaggi di posta elettronica prima che questi raggiungano la casella del destinatario, prevedendo anche l'impiego di strumenti antispam.
8.9.2	M	Filtrare il contenuto del traffico web.	Implementata	È stato adottato un firewall / proxy per filtrare il contenuto del traffico web, attraverso la definizione di una blacklist di indirizzi e contenuti.
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).	Implementata	Si è provveduto a configurare i sistemi di protezione (antivirus, firewall/proxy) per bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa (es. cab, exe).
8.10.1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	Non implementata	
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.	Non implementata	

ISTITUTO COMPRENSIVO POLO I

73013 GALATINA (LE) Piazza F. Cesari, 14

Tel: 0836566035 E-mail: leic887006@istruzione.it

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID	Livello	Descrizione	Stato	Modalità
10.1.1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	Implementata	Per gli archivi elettronici mantenuti in locale, vengono eseguite copie di backup con frequenza variabile (e sempre comunque almeno settimanale) a seconda della tipologia di dati e della criticità dei servizi collegati. Il responsabile dei sistemi informatici mantiene sempre allineata alle versioni più recenti le immagini di installazione delle applicazioni al fine di garantire il ripristino delle funzionalità dei servizi nel più breve tempo possibile. Per i servizi web, affidati in outsourcing, si è provveduto a verificare - mediante acquisizione della policy della privacy del fornitore - la rispondenza delle misure adottate dallo stesso in materia di gestione delle copie di sicurezza, ai requisiti previsti dalla normativa e alle esigenze dell'amministrazione.
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.	Non implementata	
10.1.3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	Non implementata	
10.2.1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	Non implementata	
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.	Implementata	Sono adottati idonei sistemi di protezione fisica dei supporti contenenti le copie di backup degli archivi elettronici (es. conservazione in cassaforte o in locali ad accesso controllato). Le copie di backup sono accessibili solo al responsabile della gestione privacy e al responsabile dei servizi informatici. Eventuali copie di backup conservate su servizi cloud vengono crittografate prima della trasmissione.
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.	Implementata	I supporti fisici sui quali sono mantenute le copie di sicurezza, sono mantenuti separati dalla rete.

ABSC 13 (CSC 13): PROTEZIONE DEI DATI

ABSC_ID	Livello	Descrizione	Stato	Modalità

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.	Implementata	Il responsabile della gestione privacy tiene ed aggiorna periodicamente l'elenco dei trattamenti eseguiti con strumenti elettronici, verificando che siano presenti adeguate misure di sicurezza a protezione delle banche dati e in particolar modo di quelle contenenti dati sensibili (es. password di protezione del database o crittografia della bancadati). Per i servizi web, affidati in outsourcing, si è provveduto a verificare - mediante acquisizione della policy della privacy del fornitore - la rispondenza delle misure adottate dallo stesso in materia di gestione degli archivi elettronici, ai requisiti previsti dalla normativa e alle esigenze dell'amministrazione.
13.2.1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti.	Non implementata	
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.	Non implementata	
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.	Non implementata	
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.	Non implementata	
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.	Non implementata	
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.	Non implementata	
13.6.2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	Non implementata	
13.7.1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	Non implementata	

13.8.1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Implementata	Con riguardo alla navigazione in internet, l'organizzazione, al fine di ridurre il rischio di usi impropri, non correlati alla prestazione lavorativa, ha configurato i firewall/proxy in modo da bloccare determinate operazioni quali l'accesso ai siti inseriti in blacklist o il download di file aventi determinate caratteristiche.
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.	Non implementata	