ISTITUTO OMNICOMPRENSIVO STATALE FILADELFIA

Scuola dell'Infanzia, Scuola Primaria, Scuola Secondaria di primo grado, Liceo Scientifico, IPSIA
Viale Europa – 89814 FILADELFIA (VV) – tel. 0968 724044; C.M. VVMM008008 – C.F. 96013080799 – www.omnifiladelfia.gov.it - vvmm008008@istruzione.it – vvmm008008@pec.istruzione.it

Atto di adozione prot. n. 9226/A

Filadelfia, 27 dicembre 2017

ALLEGATO 1 - Modulo implementazione Misure Minime con suggerimenti

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	L'inventario è riportato in allegato al presente documento (Inventario Hardware e Software.xlsx [scheda Hardware]) che è conservato presso l'ufficio del dirigente in apposita cartella firmato digitalmente. L'inventario elenca i dispositivi informatici collegati in rete in modo permanente o provvisorio ed è strutturato nel modo seguente: • **codice identificativo assegnato all'apparato (inventario patrimoniale);** • **descrizione breve del tipo di dispositivo;** • **MAC Address;** • **indirizzo IP** (se statico; se invece l'indirizzo IP viene assegnato dinamicamente, verrà attiva la conservazione del log del DHCP server - vedi punti 1.2.1 e 1.2.2); • **Collocazione e persona alla quale è assegnato**.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	L'elenco di cui alla misura 1.1.1 è aggiornato. L'aggiornamento dell'elenco è a carico del amministratore di

					sistema, nella fattispecie il dirigente scolastico.
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.

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 necessarie per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	L'inventario è riportato in allegato al presente documento (Inventario Hardware e Software.xlsx [scheda Software]) che è conservato presso l'ufficio del dirigente in apposita cartella che contiene tutti i documenti della scuola. L'inventario contiene: • tipologia dispositivo • nome del software • fornitore e/o marca • versione • soggetto autorizzante • eventuale data di scadenza dell'autorizzazione L'aggiornamento dell'elenco dei software è a carico del responsabile. 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 state concesse solamente agli amministratori di sistema (vedi 5.1.1)
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	Premettendo che su ciascun Personal Computer dei laboratori sono presenti due utenti e che gli allievi accedono con l'utenza "Studenti" abilitata ad effettuare operazioni ristrette (l'installazione di software non è contemplata), i responsabili di laboratorio 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 al Responsabile della transizione Digitale, che provvede affinché venga rimosso o, se valutato necessario, a che venga inserito nell'elenco.

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.	Le configurazioni standard sono quelle già previste dai Sistemi Operativi che si ritengono sufficienti a garantire un livello di sicurezza adeguato per la rete didattica. Per la rete di segreteria si prevede oltre a quanto detto al punto precedente un antivirus per la navigazione in rete. Sono utilizzate copie immagine conservate come descritto al punto 3.3.1.
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 in tal senso ai responsabili di laboratorio e di segreteria. Si procederà quindi ad eseguire il punto di ripristino del sistema più recente ed in caso di problemi ci si potrà avvalere di esperti esterni.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Non si ritiene necessario attivare immagini di ripristino poiché per i laboratori didattici lo stesso può avvenire mediante clonazione di altri HD o mediante un ripristino totale del sistema, tanto perché non esistono dati da preservare nel tempo. Alcuni software della segreteria operano con database delocalizzati rispetto ai quali non è

					necessaria l'immagine in quanto l'eventuale ripristino da crash è facilmente riparabile mediante l'intervento delle aziende fornitrici. Invece i dati ed altri software in locale, sono oggetto di backup ricorrenti a cadenza prestabilite.
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).	La rete didattica è separata da quella della segreteria. Le connessioni con le reti ministeriali avvengono con protocolli sicuri (https, ecc…).

ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ

ABSC_ID			Livello	Descrizione	Modalità di implementazione
4	1	1	M	Ad ogni modifica significativa della configurazione eseguire la ricerca delle vulnerabilità su tutti i sistemi in rete con strumenti automatici che forniscano a ciascun amministratore di sistema report con indicazioni delle vulnerabilità più critiche.	Per la segreteria si utilizza il software antivirus in aggiunta al software di scansione vulnerabilità. Per la didattica non sono necessari software specifici. I responsabili di laboratorio e gli operatori di segreteria sono informati sulla necessità di monitorare tutti i sistemi in rete, a fronte di una significativa modifica (installazione di un sistema o software nuovo, aggiornamento, modifica della configurazione) di uno o più sistemi o software.
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 operatori di verificare che il software di scansione, prima di ciascun utilizzo, sia aggiornato rispetto alle vulnerabilità.
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del	L'applicazione delle patch di vulnerabilità è schedulata dai

				software sia per il sistema operativo sia per le applicazioni.	responsabili di laboratorio e dagli operatori di segreteria. Qualora l'applicazione automatica delle patch non abbia avuto successo o provochi gravi problemi al funzionamento dei sistemi, sarà necessario bloccare l'attività di patching.
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.	I dispositivi air-gapped sono connessi solo nella rete didattica essendo la rete wi-fi di segreteria bloccata.
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 ai responsabili di laboratori e agli operatori di segreteria di verificare la risoluzione delle vulnerabilità. Nel caso non siano state trovate o applicate le patch necessarie saranno attivate le eventuali contromisure.
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.).	E' stato redatto il DPP (Documento Programmatico in materia di Privacy) per la gestione del trattamento dati e del rischio informatico in generale. Si analizzano le azioni suggerite dal report prodotto dello strumento di scansione, agendo in base alle priorità ivi indicate.
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 operatori di segreteria e ai responsabili di laboratorio.

ISTITUTO OMNICOMPRENSIVO STATALE FILADELFIA

Scuola dell'Infanzia, Scuola Primaria, Scuola Secondaria di primo grado, Liceo Scientifico, IPSIA
Viale Europa – 89814 FILADELFIA (VV) – tel. 0968 724044; C.M. VVMM008008 – C.F. 96013080799 – www.omnifiladelfia.gov.it - vvmm008008@istruzione.it – vvmm008008@pec.istruzione.it

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.	La rete didattica è strutturata in modalità peer to peer; ogni pc ha più account, i privilegi di amministrazione sono riservati al docente. La rete di segreteria è di tipo peer to peer e ogni utente ha i privilegi di amministratore ciò si rende necessario per la gestione e il controllo completo dei software, degli aggiornamenti e delle minacce.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Non è necessario registrare gli accessi nella rete di segreteria poiché vi è un rapporto 1:1 tra operatore e dispositivo. La rete didattica non presenta tale necessità.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	I documenti di nomina dei responsabili di laboratorio e degli assistenti amministrativi sono consegnati agli stessi e una copia è conservata in segreteria.
5	3	1	M	Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.	Agli operatori sono state impartite adeguate istruzioni al riguardo.
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).	Alcuni software hanno un sistema di autenticazione che obbliga agli utenti l'utilizzo di password di autenticazioni "forti", "almeno 8 caratteri di cui uno speciale + 1 numero + una maiuscola"; laddove il software non obblighi tale struttura, sarà cura degli operatori impostare una password "forte".
5	7	3	M	Assicurare che le credenziali delle utenze amministrative	Alcuni software obbligano il cambio password con cadenza

				vengano sostituite con sufficiente frequenza (password aging)	prestabilita; in alternativa il cambio verrà eseguito periodicamente dagli operatori. Misura che è già prevista obbligatoriamente dall'allegato B "Misure minime" del Codice Privacy
5	7	4	M	Impedire che credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Alcuni software sono configurati per impedire il riutilizzo delle ultime 6 password per tutti gli utenti, altrimenti sarà cura degli operatori evitare il riutilizzo di password precedenti.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	Agli operatori di segreteria e ai responsabili di laboratorio 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.	Le utenze di segreteria sono assegnate alla singola persona. Tale livello di protezione non è necessario nella rete didattica, tuttavia, ove possibile si crea un account per ogni alunno/classe.
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 devono essere gestite in modo da assicurare l'imputabilità di chi ne fa uso.	Agli operatori di segreteria e ai responsabili di laboratorio sono state impartite adeguate istruzioni al riguardo.
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Come previsto dal D.Lgs. 196/2003 Privacy, vengono raccolte in busta chiusa e conservate dal responsabile del trattamento. Le credenziali di accesso sono personali e quindi non possono essere conosciute da altri utenti.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali,	Non si utilizzano certificati digitali per l'autenticazione delle

				garantire che le chiavi private siano adeguatamente protette.	utenze di amministrazione se non quelle di sistema.

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. Risulta inoltre presente software per il rilievo della presenza di malicious software (Anti-Malware) con settaggio per l'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.
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 di segreteria. Ciò non è possibile per la rete didattica che per sua natura non può essere limitata ma deve essere estesa anche ai dispositivi personali degli alunni.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	E' stata data disposizione agli operatori di segreteria 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 di segreteria di configurare in tal senso le postazioni di lavoro. E' possibile utilizzare le group policy per Windows e MS Office. help.libreoffice.org/Common/Security_Warning o https://wiki.documentfoundation.org/Deployment_and_Migrat

					ion/it#Installazione_GPO
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	E' stata data disposizione agli operatori di segreteria 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 operatori di segreteria 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 operatori di segreteria 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.	La scuola utilizza il servizio di posta elettronica ministeriale e certificata (PEC) che include il filtro richiesto.
8	9	2	M	Filtrare il contenuto del traffico web.	L'antivirus include funzioni di filtraggio e sono state date disposizioni agli operatori di configurare il software antivirus delle postazioni di lavoro in tal senso.
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).	L'antivirus include funzioni di filtraggio e sono state date disposizioni agli operatori di configurare il software antivirus delle postazioni di lavoro in tal senso.

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.	Alcuni software che gestiscono dati da proteggere richiedono automaticamente le copie di backup pena il blocco delle funzioni. Le copie sono generalmente prodotte con cadenza periodica. Per i dati/software più importanti vengono attivati specifici sistemi di backup automatici.
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.	Il backup è effettuato sull'HD e su pen drive che sono fisicamente custodite in luoghi diversi. Può anche essere attivato un sistema di backup automatico su cloud.
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.	Si veda il punto 10.3.1

ISTITUTO OMNICOMPRENSIVO STATALE FILADELFIA

Scuola dell'Infanzia, Scuola Primaria, Scuola Secondaria di primo grado, Liceo Scientifico, IPSIA
Viale Europa – 89814 FILADELFIA (VV) – tel. 0968 724044; C.M. VVMM008008 – C.F. 96013080799 – www.omnifiladelfia.gov.it - vvmm008008@istruzione.it – vvmm008008@pec.istruzione.it

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 fisicamente controllato e protetto da password.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	L'antivirus include funzioni di filtraggio; se necessario vengono aggiunti nella blacklist gli URL da bloccare.

IL RESPONSABILE DELLA TRANSIZIONE DIGITALE
IL DIRIGENTE SCOLASTICO
Prof.ssa Maria Viscone
(Firmato digitalmente)