ISTITUTO COMPRENSIVO

SCUOLA DELL'INFA.NZIA, PRIMARIA E SECONDARIA PRIMO GRA.D0

Via Italia - Tel. 096881006 Fax 0968818921 czic813004@istreccione.it — Sito web: vs-ww.icserrastretta.it

Codice Meccanografíco:CZIC813004 _ CODICE FISCALE: 82006460792

88040 SERRASTRETTA (CZ)

Atto di adozione prot. n.4365 DEL 17/12/2019

All'Albo
Amministrazione trasparenza sez. Atti generali /Atti amm.vi
Sito web
Atti

OGGETTO: Nomina Responsabile della Transizione Digitale.

IL DIRIGENTE SCOLASTICO

VISTA la circolare AGID n. 2 del 18/04/2017 Sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante: «Misure minime di sicurezza ICT per le pubbliche amministrazioni;
VISTO il D.Lgs 165/2001"Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche";
VISTO il Codice dell'Amministrazione Digitale (CAD) di cui al D.lgs. 82/2005, come modificato dal algs. 179/2016, attuativo dell'art. 1 della Legge 124/2014 di riforma della Pubblica Amministrazione (cd. Legge Madia);
CONSIDERATO CHE le modifiche apportate al Codice dell'Amministrazione digitale dal D.lgs. 179/2016 sono finalizzate a rendere attuabile la transizione alla modalità operativa digitale per un'Amministrazione digitale e aperta;
CONSIDERATO CHE per l'attuazione della transizione digitale dell'Amministrazione, l'art.17 c. 1 del CAD prevede l'individuazione di un "Responsabile della transizione digitale" cui sono attribuiti importanti compiti decisionale e di coordinamento, dovendo garantire "l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione";
CONSIDERATO CHE il Responsabile della transizione digitale deve essere trasversale a tutta l'organizzazione in modo da poter agire su tutti gli uffici, con riferimento ai compiti relativi alla transizione digitale;
PRESO ATTO CHE i sistemi e i processi informatici dell'Istituto dovranno essere modificati ed adeguati in base al risultati dell'analisi dei processi, alla luce anche delle recenti modifiche intervenute in materia di pubblicità e trasparenza di cui al digs. 33/2013, come revisionato a seguito dell'entrata in vigore del digs. 97/2016 cd. Freedom of Information Act (FOIA);
RILEVATO CHE il Dirigente Scolastico Giuseppe Volpe è la figura apicale dell'Istituto scolastico e, come tale, di indirizzo e coordinamento per il raggiungimento degli obiettivi strategici, nonché figura individuata, alla luce delle disposizioni dell'art. 17 del CAD, per il ruolo di Responsabile della transizione digitale;

DETERMINA

per le motivazioni e le finalità di cui in premessa, di individuare, ai sensi dell'ad. 17 del Codice dell'Amministrazione Digitale, il Dirigente Scolastico GIUSEPPE VOLPE Responsabile della transizione alla modalità operativa digitale, cui sono affidati i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità.

Il presente atto non comporta impegni di spesa a carico del Bilancio Pubblico.
Il dirigente è supportato dai responsabili di laboratorio, dagli operatori di segreteria e da eventuali esperti esterni all'occorrenza incaricati.

Il Dirigente Scolastico
Giuseppe Volpe

ISTITUTO COMPRENSIVO
SCUOLA DELL'INFANZIA, PRIMARIA E SECONDARIA PRIMO GRADO
Via G. Leopardi - Tel. 096881006 **Fax** 0968818921 **- E-mail: czic813004@istruzione.it Codice Meccanografico:**CZIC813004 – **Distretto Scolastico N.12 – CODICE FISCALE:** 82006460792

Atto di adozione prot. n. 5250/viii.1 DEL 30/12/2017

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 e marcato temporalmente oppure in Conservazione a Norma. 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	1	2	S	Implementare ABSC 1.1.1 attraverso uno strumento automatico	
1	1	3	A	Effettuare il discovery dei dispositivi collegati alla rete con allarmi in caso di anomalie.	
1	1	4	A	Qualificare i sistemi connessi alla rete attraverso l'analisi del loro traffico.	
1	2	1	S	Implementare il "logging" delle operazioni del server DHCP.	
1	2	2	S	Utilizzare le informazioni ricavate dal "logging" DHCP per migliorare l'inventario delle risorse e identificare le risorse non ancora censite.	
1	**3**	**1**	**M**	**Aggiornare l'inventario quando nuovi dispositivi approvati**	L'elenco di cui alla misura 1.1.1 è aggiornato.

				vengono collegati in rete.	L'aggiornamento dell'elenco è a carico del amministratore di sistema, nella fattispecie il dirigente scolastico.
1	3	2	S	Aggiornare l'inventario con uno strumento automatico quando nuovi dispositivi approvati vengono collegati in rete.	
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.	
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.	
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.	
1	6	1	A	Utilizzare i certificati lato client per validare e autenticare i sistemi prima della connessione a una rete locale.	

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	**1**	**1**	**M**	**Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.**	L'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 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.	
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).	
2	2	3	A	Utilizzare strumenti di verifica dell'integrità dei file per verificare che le applicazioni nella "whitelist" non siano state modificate.	
2	**3**	**1**	**M**	**Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.**	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.
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.	
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.	.
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.**	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	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.	
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.	
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	2	3	S	Le modifiche alla configurazione standard devono essere effettuate secondo le procedure di gestione dei cambiamenti.	
3	**3**	**1**	**M**	**Le immagini d'installazione devono essere memorizzate offline.**	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 di 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	3	2	S	Le immagini d'installazione sono conservate in modalità protetta, garantendone l'integrità e la disponibilità solo agli utenti autorizzati.	
3	**4**	**1**	**M**	**Eseguire tutte le operazioni di amministrazione remota di server, workstation, dispositivi di rete e analoghe apparecchiature per mezzo di connessioni protette (protocolli intrinsecamente sicuri, ovvero su canali sicuri).**	La rete didattica è separata da quella della segreteria. Le connessioni con le reti ministeriali avvengono con protocolli sicuri (https, ecc…).
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.	

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.	
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.	
3	5	4	A	I controlli di integrità devono inoltre identificare le alterazioni sospette del sistema, delle variazioni dei permessi di file e cartelle.	
3	6	1	A	Utilizzare un sistema centralizzato di controllo automatico delle configurazioni che consenta di rilevare e segnalare le modifiche non autorizzate.	
3	7	1	A	Utilizzare strumenti di gestione della configurazione dei sistemi che consentano il ripristino delle impostazioni di configurazione standard.	

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	1	2	S	Eseguire periodicamente la ricerca delle vulnerabilità ABSC 4.1.1 con frequenza commisurata alla complessità dell'infrastruttura.	
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 ConfigurationEnumeration Project).	
4	2	1	S	Correlare i log di sistema con le informazioni ottenute dalle scansioni delle vulnerabilità.	
4	2	2	S	Verificare che i log registrino le attività dei sistemi di scanning delle vulnerabilità	
4	2	3	S	Verificare nei log la presenza di attacchi pregressi condotti contro target riconosciuto come vulnerabile.	
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.	
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.	
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	4	2	S	Registrarsi ad un servizio che fornisca tempestivamente le informazioni sulle nuove minacce e vulnerabilità. Utilizzandole per aggiornare le attività di scansione	
4	**5**	**1**	**M**	**Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.**	L'applicazione delle patch di vulnerabilità è schedulata dai 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	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.	
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	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.	
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.
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.	
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.	

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**	La rete didattica è strutturata in modalità peer to peer ogni pc ha

				abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi.	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	1	3	S	Assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa.	
5	1	4	A	Registrare le azioni compiute da un'utenza amministrativa e rilevare ogni anomalia di comportamento.	
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	2	2	A	Gestire l'inventario delle utenze amministrative attraverso uno strumento automatico che segnali ogni variazione che intervenga.	
5	**3**	**1**	**M**	**Prima di collegare alla rete un nuovo dispositivo sostituire le credenziali dell'amministratore predefinito con valori coerenti con quelli delle utenze amministrative in uso.**	Agli operatori sono state impartite adeguate istruzioni al riguardo.
5	4	1	S	Tracciare nei log l'aggiunta o la soppressione di un'utenza amministrativa.	
5	4	2	S	Generare un'allerta quando viene aggiunta un'utenza amministrativa.	
5	4	3	S	Generare un'allerta quando vengano aumentati i diritti di un'utenza amministrativa.	
5	5	1	S	Tracciare nei log i tentativi falliti di accesso con un'utenza amministrativa.	
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).**	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	2	S	Impedire che per le utenze amministrative vengano utilizzate credenziali deboli.	
5	**7**	**3**	**M**	**Assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza (password aging)**	Alcuni software obbligano il cambio password con cadenza prestabilità; 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	7	5	S	Assicurare che dopo la modifica delle credenziali trascorra un sufficiente lasso di tempo per poterne effettuare una nuova.	
5	7	6	S	Assicurare che le stesse credenziali amministrative non possano essere riutilizzate prima di sei mesi.	
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.	
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.	
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 debbono 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	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).	
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, garantire che le chiavi private siano adeguatamente protette.**	Non si utilizzano certificati digitali per l'autenticazione delle 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	1	3	S	Gli eventi rilevati dagli strumenti sono inviati ad un repository centrale (syslog) dove sono stabilmente archiviati.	
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.	
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.	

8	2	3	A	L'analisi dei potenziali malware è effettuata su di un'infrastruttura dedicata, eventualmente basata sul cloud.	
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	3	2	A	Monitorare l'uso e i tentativi di utilizzo di dispositivi esterni.	
8	4	1	S	Abilitare le funzioni atte a contrastare lo sfruttamento delle vulnerabilità, quali Data ExecutionPrevention (DEP), Address Space Layout Randomization (ASLR), virtualizzazione, confinamento, etc. disponibili nel software di base.	
8	4	2	A	Installare strumenti aggiuntivi di contrasto allo sfruttamento delle vulnerabilità, ad esempio quelli forniti come opzione dai produttori di sistemi operativi.	
8	5	1	S	Usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host.	
8	5	2	A	Installare sistemi di analisi avanzata del software sospetto.	
8	6	1	S	Monitorare, analizzare ed eventualmente bloccare gli accessi a indirizzi che abbiano una cattiva reputazione.	
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_Migration/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.
8	10	1	S	Utilizzare strumenti anti-malware che sfruttino, oltre alle firme, tecniche di rilevazione basate sulle anomalie di comportamento.	
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.	

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	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.	
10	1	3	A	Effettuare backup multipli con strumenti diversi per contrastare possibili malfunzionamenti nella fase di restore.	
10	2	1	S	Verificare periodicamente l'utilizzabilità delle copie mediante ripristino di prova.	

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

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	2	1	S	Utilizzare sistemi di cifratura per i dispositivi portatili e i sistemi che contengono informazioni rilevanti	
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.	
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.	
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.	
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.	
13	6	1	A	Implementare strumenti DLP (Data LossPrevention) di rete per monitorare e controllare i flussi di dati all'interno della rete in maniera da evidenziare eventuali anomalie.	
13	6	2	A	Qualsiasi anomalia rispetto al normale traffico di rete deve essere registrata anche per consentirne l'analisi off line.	
13	7	1	A	Monitorare il traffico uscente rilevando le connessioni che usano la crittografia senza che ciò sia previsto.	
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.
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.	