Direttore tecnico
Cassese Felice
Via Alcide De Gasperi, 34-A
Palma Campania (NA)
Abilitazione professionale n. 32025

Spett.le
Dirigente Scolastico
Direzione Didattica "A. Moro"
Via Cesare Pascarella, 20
05100 – Terni – (TR)
Codice fiscale: 80004550556

Prot.n. 6312/B15a

Terni, 30/10/2018

IL RESPONSABILE ALLA TRANSIZIONE DIGITALE

VISTO l'art. 17 del C.A.D. vigente;
VISTO l'incarico del responsabile alla transizione digitale prot. n. 1926/B15 del 10/04/2018;
VISTA la circolare M.I.U.R. riferita alle misure minime di sicurezza ICT per le pubbliche amministrazioni prot. n. 3015/AOODGCASIS del 20/12/2017;
VISTA la CIRCOLARE AGID del 18 aprile 2017, n. 2/2017;
VISTA l'esigenza di compilare il modello di implementazione;
VISTI gli adempimenti da adeguare indicati nel modello di implementazione prot. n. 1929/B15 del 10/04/2018.

APPROVA

Il seguente adeguamento al modulo di implementazione:

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
1	1	1	M	Implementare un inventario delle risorse attive correlato a quello ABSC 1.4	E' stato creato un elenco in formato elettronico e cartaceo delle apparecchiature elettroniche come personal computer, notebook, access point, stampanti, fotocopiatrici ecc. L'elenco è comprensivo

					di IP statici.
1	3	1	M	Aggiornare l'inventario quando nuovi dispositivi approvati vengono collegati in rete.	Qualora si dovesse acquisire un nuovo dispositivo, l'inventario delle risorse attive dovrà essere aggiornato. Ad oggi l'inventario risulta aggiornato.
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.	L'inventario viene gestito attraverso una lista di device comprendendo gli IP associati ad ogni dispositivo e i MAC Address

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

ABSC_ID			Livello	Descrizione	Modalità di implementazione
2	1	1	M	Stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server, workstation e laptop di vari tipi e per diversi usi. Non consentire l'installazione di software non compreso nell'elenco.	E' presente un elenco di software autorizzati comprensivo di versioni suddiviso per categorie.
2	3	1	M	Eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato.	L'amministratore di sistema nominato con prot. n. 5562/Fp del 08/10/2018 verifica l'esecuzione delle scansioni mensili sui sistemi operativi per rilevare la presenza di software non autorizzati.

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.	Sono state configurare tutte le macchine attivando una configurazione standard di protezione nonché antivirus centralizzato e firewall hardware.

3	2	1	M	Definire ed impiegare una configurazione standard per workstation, server e altri tipi di sistemi usati dall'organizzazione.	E' stato creato un file dove sono state indicate le configurazioni standard delle postazioni presenti in segreteria.
3	2	2	M	Eventuali sistemi in esercizio che vengano compromessi devono essere ripristinati utilizzando la configurazione standard.	Punti di ripristino attivi settimanalmente su tutte le macchine presenti in segreteria.
3	3	1	M	Le immagini d'installazione devono essere memorizzate offline.	Disco di ripristino in formato DvD-ROM
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).	L'amministrazione non utilizza desktop remoto pertanto non necessita di protocolli SSH, saltuariamente riceve assistenza tecnica remota attraverso il software team viewer, la password cambia ad ogni avvio e il software non si avvia automaticamente

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.	Installato il software LanSweeper per la ricerca delle vulnerabilità dei sistemi in rete
4	4	1	M	Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza.	Su tutte le postazioni è presente kaspersky office security, con impostazione automatica sugli aggiornamenti
4	5	1	M	Installare automaticamente le patch e gli aggiornamenti del software sia per il sistema operativo sia per le applicazioni.	Sono stati attivati gli aggiornamenti automatici del sistema operativo
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.	Tutti i device sono collegati alla rete
4	7	1	M	Verificare che le vulnerabilità emerse dalle scansioni siano state risolte sia per mezzo di patch, o implementando	L'amministratore di rete redige un report

				opportune contromisure oppure documentando e accettando un ragionevole rischio.	qualora ci fossero delle vulnerabilità emerse e come sono state risolte.
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 creato un elenco con i livelli di rischio suddiviso con Minimo – Medio - Alto, documento acquisito con prot. n. 5563/Fp del 08/10/2018
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.	Il livello del server risulta con rischio "Alto" sulla ."Medio" sulle postazione PdL.

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.	E' stato creato un account administrator e user limitato.
5	1	2	M	Utilizzare le utenze amministrative solo per effettuare operazioni che ne richiedano i privilegi, registrando ogni accesso effettuato.	Account utente limitato pertanto qualora si dovessero apportare modifiche al sistema sarà necessario l'intervento dell'amministratore di reti.
5	2	1	M	Mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata.	E' stato creato un elenco elettronico e cartaceo degli utenti attivi che utilizzano le postazioni associandole ai nominativi.
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.	E' stato creato un account user con password su ogni singola postazione
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).	E' stata inserita all'utente amministratore una password di 14 caratteri
5	7	3	M	Assicurare che le credenziali delle utenze amministrative	Le password saranno

				vengano sostituite con sufficiente frequenza (password aging).	sostituite con cadenza trimestrale
5	7	4	M	Impedire che le credenziali già utilizzate possano essere riutilizzate a breve distanza di tempo (password history).	Non saranno inserite password già utilizzate in passato, è stato configurato il sistema operativo in modo da non consentire il salvataggio di una vecchia password.
5	10	1	M	Assicurare la completa distinzione tra utenze privilegiate e non privilegiate degli amministratori, alle quali debbono corrispondere credenziali diverse.	E' stato differenziato l'utente amministratore con l'utente user
5	10	2	M	Tutte le utenze, in particolare quelle amministrative, debbono essere nominative e riconducibili ad una sola persona.	E' stato nominato l'amministratore di sistemi interno per la gestione delle credenziali di accesso di tipo admin.
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.	Come al punto 5.10.2
5	11	1	M	Conservare le credenziali amministrative in modo da garantirne disponibilità e riservatezza.	Le credenziali admin sono custodite dall'amministratore informatico.
5	11	2	M	Se per l'autenticazione si utilizzano certificati digitali, garantire che le chiavi private siano adeguatamente protette.	Non vengono utilizzate autenticazioni con certificati digitali

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.	L'istituto utilizza l'antivirus Kaspersky office security suite, centralizzato
8	1	2	M	Installare su tutti i dispositivi firewall ed IPS personali.	Firewall hardware presente
8	3	1	M	Limitare l'uso di dispositivi esterni a quelli necessari per le attività scolastiche.	L'accesso ai dati sensibili è bloccato dal firewall pertanto la rete di segreteria non è accessibile se

					non attraverso il firewall.
8	7	1	M	Disattivare l'esecuzione automatica dei contenuti al momento della connessione dei dispositivi removibili.	Esecuzione automatica disattivata
8	7	2	M	Disattivare l'esecuzione automatica dei contenuti dinamici (e.g. macro) presenti nei file.	Marco disattivate
8	7	3	M	Disattivare l'apertura automatica dei messaggi di posta elettronica.	L'Istituto legge la posta on-line, quindi non utilizza software di posta elettronica
8	7	4	M	Disattivare l'anteprima automatica dei contenuti dei file.	Anteprima disattivata
8	8	1	M	Eseguire automaticamente una scansione anti-malware dei supporti rimuovibili al momento della loro connessione.	Il personale effettua la scansione sui supporti rimovibili attraverso Kaspersky
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.	Filtro antispam attivo
8	9	2	M	Filtrare il contenuto del traffico web.	Web filtering attivo
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).	Il traffico web è monitorato dall'antivirus e dal firewall

ABSC 10 (CSC 10): COPIE DI SICUREZZA

ABSC_ID			Livello	Descrizione	Modalità di implementazione
10	1	1	M	Effettuare almeno settimanalmente una copia di sicurezza almeno delle informazioni strettamente necessarie per il completo ripristino del sistema.	E' stata abilitata la copia di sicurezza di windows pianificata settimanalmente
10	3	1	M	Assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti ovvero mediante cifratura. La codifica effettuata prima della trasmissione consente la remotizzazione del backup anche nel cloud.	Sono stati attivati i punti di ripristino sul NAS protetti da password
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.	I contenuti sono accessibili solo all'interno della rete.

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	Sono stati attivati i backup dei dati

				segnatamente quelli ai quali va applicata la protezione crittografica	protetti da password.
13	8	1	M	Bloccare il traffico da e verso url presenti in una blacklist.	Url filtering attivi

Considerati gli adempimenti relativi alle misure minime di sicurezza nonché dell'adeguamento del modello di implementazione emanato dall'AGId, si procede alla verifica di tali adempimenti il giorno 30 Ottobre 2018 alle ore 8:30 presso la Direzione Didattica "A. Moro" di Terni (TR).

Pertanto si attesta che il predetto Istituto scolastico risulta **adeguato rispetto alle norme vigenti sulla sicurezza informatica** rispettando i criteri minimi come indicato dalla circolare M.I.U.R. prot. n. 3015/AOODGCASIS del 20/12/2017 pagina n. 3 "Livelli di applicazione". La verifica termina alle ore 12:30 con esito positivo.

Il Dirigente Scolastico
Prof.ssa Maria Rosaria De Fusco
Firmato digitalmente

Responsabile alla transizione digitale
Direttore Tecnico Cassese Felice
Firmato Digitalmente