

**ISTITUTO
COMPRESIVO
« Tommasone-Alighieri »**

**PIANO DI
IMPLEMENTAZIONE
Misure Minime di Sicurezza
ICT
per le Pubbliche Amministrazioni**

aggiornamento 2023

AMBITI DI INTERVENTO

- **Formazione interna**
- **Coinvolgimento della Comunità scolastica**

REFERENTE:
Gennaro CAMPOREALE

- **Responsabile Piano di implementazione: Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni**

**DIRETTIVA del
Presidente del
Consiglio dei Ministri
del 1 agosto 2015**

FORMAZIONE INTERNA

PERSONALE ATA: amministrativi

- aggiornare l'inventario dei dispositivi
- Correzione contro le vulnerabilità
- Difese contro i malware
- Protezione dati e copie sicurezza

MISURE MINIME DI SICUREZZA: SCHEDA DI SINTESI STATO DI ATTUAZIONE GIUGNO 2023

LIVELLO DI SICUREZZA: MEDIO-ALTO

MISURE MINIME DI SICUREZZA ICT	DESCRIZIONE MODALITA' DI IMPLEMENTAZIONE	DESCRIZIONE COMPITI ASSEGNATI	STATO DI ATTUAZIONE
1. INVENTARIO DEI DISPOSITIVI 2. INVENTARIO DEI SOFTWARE	<i>implementare e aggiornare l'inventario dei dispositivi</i>	Per ogni dispositivo fisso e mobile, indicare: <ul style="list-style-type: none"> a. Ubicazione e Nominativo della persona a cui è assegnato il dispositivo o del referente per i dispositivi dei laboratori. b. Tipologia, marca e n. inventario c. Sistema operativo installato, IP assegnato, software installati. d. Software per la protezione, valutazione e correzione continua delle vulnerabilità e difese contro i malware 	Uffici 12 ³ 45 Laboratori 12 ³ 45 Dispositivi mobili 12 ³ 45

P.S. l'inventario dei dispositivi è in situazione di continuo work progress: viene aggiornato periodicamente con l'arrivo di nuovi dispositivi.

E' necessario procedere con l'aggiornamento del registro

MISURE MINIME DI SICUREZZA ICT	DESCRIZIONE MODALITA' DI IMPLEMENTAZIONE	DESCRIZIONE COMPITI ASSEGNATI	STATO DI ATTUAZIONE
<p>3. VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITA'</p> <p>4. DIFESE CONTRO I MALWARE</p>	<p><i>Eeguire periodicamente la ricerca delle vulnerabilità</i></p> <p><i>Assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati</i></p>	<p>1. Assicurarsi che:</p> <p>a. Il sistema operativo sia aggiornato.</p> <p>b. La propria postazione di lavoro sia dotata di antivirus e anti-Malware e che questo sia aggiornato per una periodica scansione.</p> <p>2. Scansionare periodicamente per la ricerca virus le postazioni e dispositivi di lavoro</p> <p>3. Usare con molta cautela supporti removibili quali chiavette usb e/o hard disk esterni: al momento della connessione di un supporto removibile avviare una scansione completa dello stesso attraverso il software antivirus</p>	<p>Uffici 12345</p> <p>Laboratori 12345</p> <p>Dispositivi mobili 12345</p> <p>Uffici 12345</p> <p>Laboratori 12345</p> <p>Dispositivi mobili 12345</p> <p>Uffici 12345</p> <p>Laboratori 12345</p> <p>Dispositivi mobili 12345</p> <p>Uffici 12345</p> <p>Laboratori 12345</p> <p>Dispositivi mobili 12345</p>

	<p><i>usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host</i></p> <p><i>Bloccare il traffico da e verso url presenti in una blacklist</i></p>	<p>a. disattivare l'apertura automatica dei messaggi b. disattivare l'anteprima automatica dei contenuti dei file. c. filtrare il contenuto dei messaggi prima che questi raggiungano la casella del destinatario, prevedendo l'impiego di strumenti antispam d. non dare seguito all'apertura di file non attesi, dalla dubbia provenienza o che giungano da caselle non note e. Non installare software sulle proprie postazioni di lavoro, soprattutto se a seguito di sollecitazioni via e-mail f. Non dare seguito alle richieste incluse nei messaggi: nel caso in cui le richieste provengano da parte del personale tecnico dell'Amministrazione, verificare attentamente il contesto: l'email era attesa? Il software da installare ha un fine specifico? Il mittente è corretto?</p> <p>Nei laboratori didattici frequentati dai minori, attivare un antivirus con funzioni di filtraggio e una blacklist con gli URL da bloccare.</p>	<p>Uffici 12345</p> <p>Laboratori 12345 Dispositivi mobili 12345</p>
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------

MISURE MINIME DI SICUREZZA ICT	DESCRIZIONE MODALITA' DI IMPLEMENTAZIONE	DESCRIZIONE COMPITI ASSEGNATI	STATO DI ATTUAZIONE
<p>5. USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE</p>	<p><i>Assegnare a ciascuna utenza solo i privilegi necessari per svolgere le attività previste per essa e conservare le credenziali in modo da garantirne disponibilità e riservatezza</i></p> <p><i>Per le utenze amministrative, utilizzare credenziali di elevata robustezza</i></p>	<p>Le credenziali saranno raccolte in busta chiusa e conservate dal responsabile del trattamento. Per quanto concerne i prodotti Axios le credenziali sono gestite all'interno della base dati, l'accesso è consentito solo tramite i programmi Axios</p> <p>1. Assicurarsi che: le proprie password di posta e strumenti di lavoro siano sicure:</p> <p>a. <i>Complesse (presenza di caratteri maiuscoli, minuscoli, numerici e speciali)</i></p> <p>b. <i>Non facilmente individuabili</i></p> <p>c. <i>Diverse per servizi distinti</i></p> <p>d. <i>Modificabili con cadenza prestabilita, ponendo attenzione che al momento della modifica, non siano apportate solo piccole modifiche come ad esempio numerazioni progressive</i></p> <p>2. Non salvare le password nel browser di navigazione</p> <p>3. Non usare l'account di lavoro per registrarsi in internet per fini non riconducibili alla sfera di lavoro.</p>	<p>Uffici 123³45</p> <p>Provvedere all'aggiornamento</p> <p>Uffici 123⁴5</p>

MISURE MINIME DI SICUREZZA ICT	DESCRIZIONE MODALITA' DI IMPLEMENTAZIONE	DESCRIZIONE COMPITI ASSEGNATI	STATO DI ATTUAZIONE
6. COPIE DI SICUREZZA		<ul style="list-style-type: none"> a. Effettuare almeno settimanalmente una copia di sicurezza tramite il sistema automatico Axios b. Effettuare backup del proprio dispositivo riguardanti sistema operativo, applicazioni software e parte dati 	Uffici 12345
7. PROTEZIONE DATI		Effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza ai quali va applicata la protezione crittografica	Uffici 12345

**ISTITUTO
COMPENSIVO
« Tommasone-Alighieri »**



fgic876009@istruzione.it



www.tommasone-alighieri.edu.it

Gennaro CAMPOREALE