

PIANO DI IMPLEMENTAZIONE

Misure minime di sicurezza ICT per le Pubbliche Amministrazioni

NORMATIVA DI RIFERIMENTO:
DIRETTIVA del Presidente del Consiglio dei Ministri del 1
agosto 2015

FINALITA':
migliorare la sicurezza dei sistemi informatici
scolastici attraverso «misure minime di sicurezza ICT»

Misure minime di sicurezza ICT



AREA DI INTERVENTO	MISURE MINIME DI SICUREZZA	LIVELLO DI APPLICAZIONE
<p>Le misure riportate sono un estratto del modulo di Implementazione</p>		<p>Minimo: sufficiente per tutte le Istituzioni</p> <p>Standard: come base di riferimento nella maggior parte dei casi</p> <p>Avanzato: adottato dalle organizzazioni maggiormente esposte ai rischi, e visto come obiettivo di miglioramento per tutte le istituzioni</p>
<p>1. INVENTARIO DEI DISPOSITIVI</p>	<p>–gestire l’inventario delle risorse di tutti i sistemi collegati alla rete e dei dispositivi di rete stessi, registrando almeno l’indirizzo IP</p>	<p>minimo</p>
<p>2. INVENTARIO DEI SOFTWARE</p>	<p>–stilare un elenco di software autorizzati e relative versioni necessari per ciascun tipo di sistema, compresi server</p> <p>–non consentire l’installazione di software non compreso nell’elenco</p> <p>–eseguire regolari scansioni sui sistemi al fine di rilevare la presenza di software non autorizzato</p>	<p>minimo</p>

Misure minime di sicurezza ICT



AREA DI INTERVENTO	MISURE MINIME DI SICUREZZA	LIVELLO DI APPLICAZIONE
3. PROTEZIONE DELLE CONFIGURAZIONI DI HARDWARE E SOFTWARE	<ul style="list-style-type: none">-utilizzare configurazioni sicure standard per la protezione dei sistemi operativi-utilizzare strumenti di verifica dell'integrità dei file per assicurare che i file critici del sistema non siano stati alterati	<p>minimo</p> <p>standard</p>
4. VALUTAZIONE E CORREZIONE DELLA VULNERABILITA'	<ul style="list-style-type: none">-eseguire periodicamente la ricerca delle vulnerabilità con frequenza commisurata alla complessità-assicurare che gli strumenti di scansione delle vulnerabilità utilizzati siano regolarmente aggiornati con tutte le più rilevanti vulnerabilità di sicurezza	<p>Standard</p> <p>minimo</p>

Misure minime di sicurezza ICT



AREA DI INTERVENTO	MISURE MINIME DI SICUREZZA	LIVELLO DI APPLICAZIONE
5.USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE	-limitare i privilegi di amministrazione ai soli utenti che abbiano le competenze adeguate e la necessità operativa di modificare la configurazione dei sistemi	Minimo
	-assegnare a ciascuna utenza amministrativa solo i privilegi necessari per svolgere le attività previste per essa	
	-mantenere l'inventario di tutte le utenze amministrative, garantendo che ciascuna di esse sia debitamente e formalmente autorizzata	Avanzato
	-utilizzare sistemi di autenticazione con credenziali di elevata robustezza per tutti gli accessi amministrativi, impedendo credenziali deboli	standard
	-assicurare che le credenziali delle utenze amministrative vengano sostituite con sufficiente frequenza	
	-impedire che credenziali già utilizzate posano essere riutilizzate a breve distanza di tempo (non prima dei sei mesi)	

Misure minime di sicurezza ICT



AREA DI INTERVENTO	MISURE MINIME DI SICUREZZA	LIVELLO DI APPLICAZIONE
8.DIFESA CONTRO I MALWARE	-installare su tutti i sistemi connessi alla rete locale strumenti atti a la presenza e bloccare l'esecuzione di malware (antivirus locali).Tali strumenti siano mantenuto aggiornati in modo automatico	Minimo
	-limitare l'uso di dispositivi esterni a quelli necessari per le attività aziendali (amministrative e didattica)	Standard
	-usare strumenti di filtraggio che operano sull'intero flusso del traffico di rete per impedire che il codice malevolo raggiunga gli host	Minimo
	-disattivare l'apertura automatica dei messaggi di posta elettronica	
	-disattivare l'anteprima automatica dei file	
	-bloccare nella posta elettronica e nel traffico web i file la cui tipologia non è strettamente necessaria per l'organizzazione ed è potenzialmente pericolosa	minimo

Misure minime di sicurezza ICT




AREA DI INTERVENTO	MISURE MINIME DI SICUREZZA	LIVELLO DI APPLICAZIONE
10.COPIE DI SICUREZZA	<ul style="list-style-type: none">-effettuare almeno settimanalmente una copia di sicurezza delle informazioni strettamente necessarie per il completo ripristino del sistema-effettuare procedure di backup del sistema operativo, delle applicazioni e della parte dati-assicurare la riservatezza delle informazioni contenute nelle copie di sicurezza mediante adeguata protezione fisica dei supporti e mediante cifratura	<p>Minimo</p> <p>Avanzato</p> <p>minimo</p>
13.PROTEZIONE DEI DATI	<ul style="list-style-type: none">-effettuare un'analisi dei dati per individuare quelli con particolari requisiti di riservatezza ai quali va applicata la protezione crittografica-utilizzare sistemi di cifratura per i dispositivi e i sistemi che contengono informazioni rilevanti-bloccare il traffico da e verso url presenti in una blacklist	<p>minimo</p>




I.C. "Tommasone-Alighieri"

Grazie

 Gennaro Camporeale, Tiziana Boscolo

 fgic876009@istruzione.it

 <https://www.tommasone-alighieri.edu.it/>