Istituto Comprensivo di Medesano

Via De Gasperi 2 — tel 0525.420.403
43014 Medesano (PR) — fax 0525.422.659
C.M. PRIC80900A — mail pric80900a@istruzione.it
C.F. 92103030349 — web www.icmedesano.edu.it

Regolamento tecnico

Uso del computer, della rete, di internet e della posta elettronica

L'analisi ha rilevato che principali criticità non sono dovute a ragioni hardware o software ma di natura sociale (ingegneria sociale – rispetto delle regole) e procedurale. Si consiglia a tal proposito un corso di formazione per i dipendenti affinché gestiscano correttamente strumenti e procedure e rispettino le nuove regole.

Computer, rete e autenticazioni

1. I sistemi operativi e tutti i software (online o installato) devono essere aggiornati alle ultime versioni stabili e soggetti ad aggiornamenti automatici, continui e costanti;
2. Ogni singola postazione, con accesso tramite autenticazione, deve essere dedicata a un singolo dipendente con profilo personale.
3. La gestione delle password (di rete, screen saver, email e gestionali) deve essere a norma di legge con cambio automatico obbligatorio ogni 6 mesi;
4. Le installazioni di antivirus, firewall e gestionali eventualmente anche per la posta elettronica (Ok webmail) devono essere su server;
5. Creazione di policy di backup strutturata con procedure di ripristino per i singoli computer di rete;
6. La gestione dei nuovi utenti deve avvenire tramite la distribuzione delle password in busta chiusa oppure attraverso la distribuzione di una password generica con cambio obbligatorio al primo accesso;
7. La gestione degli utenti scaduti deve avvenire tramite un responsabile il quale li deve disattivare e cancellare. Il sistema deve generare avvisi per profili non

utilizzati per 6 mesi e permettere lo scarico dei dati per ogni profilo in formato CSV (da richiedere all'istituto);

8. La gestione dei dati sensibili deve avvenire tramite l'uso di una periferica esterna di memorizzazione con la cifratura automatica dei dati e backup dedicato. Il cambio password per l'utente che gestisce i dati sensibili è pari a 3 mesi;
9. Creazione di un documento cartaceo con tutte le password da tenere in cassaforte con registro, sempre cartaceo, che tenga traccia suo utilizzo;

Gestione email

1. Le utenze mail devono essere gestite con gli stessi criteri dei profili di rete, quindi password a norma di legge, cambiamento ogni 6 mesi e distribuzione o con busta chiusa o tramite il cambiamento al primo accesso;
2. I nomi utenti delle email devono essere personali (es: m.rossi@dominio.it; mario.rossi@dominio.it; ecc…) e non per ruolo (dirigente@domino.it, personale@dominio.it, dsga@dominio.it, ecc…);
3. I browser web devono sempre essere aggiornati, la navigazione e le mail devono essere protette da antivirus e firewall e, in caso di gestione di dati sensibili su risorse esterne (cloud, webmail o simili), l'operatore deve verificare di essere in HTTPS. Il salvataggio automatico di password deve essere disabilitato e si consiglia la navigazione in incognito.

Sito web

1. L'Aggiornamento del gestionale web e di tutte le stensioni installate devono essere alle ultime release stabili;
2. Generazione articolo privacy e apertura del relativo link al primo accesso di ogni nuovo utente;
3. Generazione articolo cookie;
4. Generazione barra granulare dei cookie (l'utente sceglie quale cookie attivare);
5. Gestione dei consensi della privacy degli utenti (il sistema deve tener traccia dei consensi).