All. 3 -Piano Strategico di Sicurezza Informatica (PSSI)

Istituto di Istruzione Secondaria Superiore [Nome del Liceo]

1. Obiettivi e Finalità

Il presente documento definisce le linee guida per garantire la riservatezza, l'integrità e la disponibilità dei dati e delle infrastrutture digitali del Liceo. Il piano si applica a personale docente, ATA, studenti e collaboratori esterni.

2. Architettura della Rete e Protezione dei Dati

La rete scolastica è suddivisa in tre segmenti isolati per prevenire movimenti laterali di eventuali minacce:

1. **Rete Amministrativa:** Accesso riservato alla segreteria e alla dirigenza (massimo livello di restrizione).
2. **Rete Didattica:** Laboratori e LIM, protetta da sistemi di filtraggio contenuti.
3. **Rete Guest/Wi-Fi Studenti:** Accesso limitato con autenticazione tramite credenziali personali.

Misure Tecniche Implementate:

- **Firewall Next-Generation (NGFW):** Per il monitoraggio del traffico e la prevenzione delle intrusioni (IPS).
- **Antivirus Centralizzato:** Installato su ogni endpoint (PC di segreteria, laptop docenti).
- **Backup (Regola 3-2-1):** Tre copie dei dati, su due supporti diversi, di cui una offline o in cloud crittografato.

3. Gestione delle Identità e degli Accessi

L'accesso ai servizi digitali (Registro Elettronico, Google Workspace/Microsoft 365) segue il principio del **minimo privilegio**.

- **Password Policy:** Lunghezza minima di 12 caratteri, inclusione di simboli e numeri. Cambio obbligatorio in caso di sospetta violazione.
- **MFA (Autenticazione a due fattori):** Obbligatoria per gli amministratori di sistema e caldamente raccomandata per il personale docente sul Registro Elettronico.
- **De-provisioning:** Disattivazione immediata degli account al termine del ciclo di studi o del rapporto lavorativo.

4. Sicurezza nel Lavoro Agile e Didattica a Distanza

Per l'utilizzo di dispositivi personali (BYOD) o l'accesso da remoto:

- È vietato memorizzare dati sensibili (es. verbali, diagnosi 104) su dispositivi personali non protetti da cifratura.
- L'accesso ai server della segreteria deve avvenire esclusivamente tramite **VPN (Virtual Private Network)**.

5. Formazione e Consapevolezza

Il fattore umano è l'anello più debole. Il Liceo si impegna a:

- Organizzare corsi di formazione ;
- Pubblicare una guida rapida per gli studenti sull'uso etico della rete e la prevenzione del cyberbullismo.

6. Piano di Risposta agli Incidenti (Incident Response)

In caso di sospetta violazione (es. attacco Ransomware o smarrimento di un dispositivo):

1. **Segnalazione:** L'utente informa immediatamente l'Animatore Digitale o il Team dell'Innovazione.
2. **Isolamento:** Disconnessione immediata del dispositivo dalla rete Wi-Fi/Ethernet.
3. **Valutazione:** Analisi dell'entità del danno e verifica se sussiste l'obbligo di notifica al Garante Privacy (Data Breach) entro 72 ore, in conformità al GDPR.

Tabella dei Ruoli e Responsabilità

Ruolo	Responsabilità Principale
Dirigente Scolastico	Responsabile legale e titolare del trattamento dati.
Animatore Digitale	Coordinamento tecnico e attuazione delle misure di sicurezza.
Personale ATA	Custodia delle credenziali di accesso ai dati amministrativi.
Docenti	Vigilanza sull'uso corretto dei dispositivi in aula.

Nota per la pubblicazione: Prima di pubblicare il documento, assicurati di aver inserito i nomi specifici dei responsabili e di aver verificato la conformità con il tuo **DPO (Data Protection Officer)**.