ISTITUTO COMPRENSIVO "F. SEVERI - MANCINI"
Via Bari 15 -74012 CRISPIANO (TA)
C.F. 90283590736 - C.M. TAIC874002
Tel. 099616078 (segreteria) - Tel. 099611371 (presidenza)
Peo: taic874002@istruzione.it - Pec: taic874002@pec.istruzione.it

Piano di Formazione del Personale Scolastico sugli Obblighi NIS2

Istituzione Scolastica: ISTITUTO COMPRENSIVO "F. SEVERI - MANCINI"
Anno Scolastico: 2025-2026

1. Finalità del Piano

La Direttiva NIS2 richiede che il personale scolastico sia adeguatamente formato sui rischi informatici.
Il piano mira a sviluppare consapevolezza, capacità di riconoscere minacce e applicare comportamenti sicuri.

2. Obiettivi della formazione

Obiettivi generali:
• Rafforzare la cultura della sicurezza informatica.
• Ridurre gli incidenti causati da errore umano.
• Garantire conformità agli obblighi NIS2.

Obiettivi specifici:
• Riconoscere phishing e social engineering.
• Adottare MFA e password sicure.
• Proteggere dati personali degli studenti.
• Conoscere le procedure interne ICT.
• Gestire correttamente strumenti digitali e BYOD.

3. Destinatari

• Docenti
• Personale ATA
• DSGA
• Dirigente Scolastico
• Animatore Digitale
• Amministratore di Sistema
• Referente Cybersecurity
• Referente Cyberbullismo

4. Contenuti Formativi

Modulo 1 – Introduzione alla NIS2
• Ruolo della scuola nella sicurezza digitale
• Obblighi e responsabilità del personale

Modulo 2 – Cybersecurity di base
• Malware, ransomware, minacce più comuni

Modulo 3 – Credenziali e MFA
• Password policy scolastica
• Uso dell'autenticazione a più fattori

Modulo 4 – Uso sicuro degli strumenti digitali
• Google Workspace / Microsoft 365
• Registro elettronico e segreteria digitale

Modulo 5 – Phishing e Social Engineering
• Indicatori di email sospette
• Esercitazioni e simulazioni

Modulo 6 – Privacy e protezione dei minori
• GDPR e dati particolari
• Regole BYOD per docenti e ATA

Modulo 7 – Incident Response
• Cosa fare in caso di sospetto attacco
• Coinvolgimento del DPO e del personale ICT

Modulo 8 – Continuità operativa
• RTO, RPO
• Buone pratiche di backup e archiviazione

5. Modalità di Erogazione
• Incontri periodici in presenza o online
• Attività online in asincrono
• Moduli brevi di microlearning
• Simulazioni phishing annuali
• Quiz di verifica
• Poster e campagne informative

6. Durata e Frequenza
• Durata minima annuale: 6 ore
• 2 ore → policy e NIS2
• 2 ore → phishing, password, MFA
• 2 ore → privacy, incident response
• Aggiornamenti straordinari in caso di incidenti gravi o nuove tecnologie

7. Valutazione della Formazione
La verifica comprende:
• Quiz online
• Simulazioni phishing
• Compilazione registro formazione
• Attestazione finale

8. Ruoli e Responsabilità
• DS: supervisione generale
• DSGA: coordinamento ATA
• Animatore Digitale: supporto formativo
• Amministratore di Sistema: aspetti tecnici
• DPO: aspetti privacy

9. Tracciamento e Conservazione

La scuola conserva:

- Registro formazione cybersecurity
- Verbali delle attività
- Presenze
- Risultati test e simulazioni

Conservazione minima: 5 anni.

10. Allegati

A1 – Registro formazione cybersecurity (modello)
A2 – Verbale attività formativa (modello)
A3 – Simulazione phishing (modello)
A4 – Quiz di verifica (modello)
A5 – Poster informativi

I suddetti allegati saranno compilati e registrati nel corso dell'anno scolastico di riferimento.

IL DIRIGENTE SCOLASTICO
prof.ssa Sabrina LEPRARO

Firmato digitalmente da:
Lepraro Sabrina
Firmato il 29/12/2025 15:54
Seriale Certificato: 4807921
Valido dal 28/08/2025 al 28/08/2028
InfoCamere Qualified Electronic Signature CA

A1 – Registro Formazione Cybersecurity (modello)

Data	Titolo Formazione	Formatore	Personale Partecipante	Esito / Note

A2 – Verbale Attività Formativa (modello)

Data attività formativa:
Titolo della formazione:
Formatore / Relatore:
Destinatari: Docenti / ATA / Altro

Contenuti trattati
- Introduzione alla NIS2
- Minacce informatiche comuni
- Phishing e social engineering
- Password policy e MFA
- Procedure interne di sicurezza

Valutazione dell'attività:
Note:

Firma Formatore
Firma DS

A3 – Modello per Simulazione di Phishing

Obiettivo della simulazione
Valutare la capacità del personale di riconoscere email fraudolente.

Tipologia di email simulata
• Richiesta urgente di cambio password
• Notifica falsa del registro elettronico
• Email con link sospetto
• Allegato malevolo simulato

Indicatori valutati
• Click su link
• Apertura allegato
• Segnalazione corretta al referente ICT
• Comportamento generale del personale

Risultati (da compilare)
Percentuale di utenti che hanno riconosciuto la minaccia: _____%
Percentuale di utenti che hanno aperto il link/allegato: _____%
Azioni correttive previste: _____

A4 – Quiz di Verifica Competenze Cybersecurity (modello)

Domande a risposta multipla:
1. Qual è il segnale principale di un'email di phishing?
• Richiesta urgente di compiere un’azione
• Messaggio da un collega conosciuto
• Allegato in PDF sicuro

2. Cosa indica MFA?
• Multi-Factor Authentication
• Mail Filtering Automatico
• Mobile File Access

3. Cosa devi fare se noti un accesso sospetto?
• Segnalarlo al referente ICT
• Ignorarlo
• Aspettare e vedere se succede ancora

Spazio risposte
1. _____
2. _____
3. _____

A5 – Poster Informativi Cybersecurity per la Scuola

Regole fondamentali di sicurezza informatica
- Non aprire email sospette
- Verifica sempre il mittente
- Non condividere le credenziali
- Usa password robuste
- Attiva e usa la MFA
- Non collegare chiavette USB sconosciute
- Proteggi i dati degli studenti
- Segnala immediatamente qualsiasi anomalia

Contatto interno per la sicurezza
Referente ICT:
Amministratore di Sistema:
Email per la segnalazione incidenti: