SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

SERICS
CYBERSECURITY
ACADEMY

ATTIVITÀ TRAIN THE TRAINERS

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

I corsi per i formatori hanno l'obiettivo di formare profili professionali che abbiano le principali competenze e conoscenze del Cybersecurity Educator previsto dal Framework ECSF di ENISA, calibrato ad un livello e-CF più basso nella competenza E.8. Information Security Management, considerando che si tratta di corsi prevalentemente pensati per diffondere consapevolezza.
Al termine del corso, i formatori sapranno identificare le esigenze di cybersecurity del target, progettare programmi di apprendimento mirati, sviluppare o utilizzare esercitazioni, erogare test di valutazione e scegliere approcci pedagogici appropriati.

I CORSI:

TRAIN THE TRAINERS RIVOLTA A DOCENTI DI STUDENTI K0-K8 **04**

Percorsi progettati con l'obiettivo primario di creare consapevolezza in merito alle criticità dovute a una scarsa attenzione alla gestione dei dati.

TRAIN THE TRAINERS RIVOLTA A DOCENTI, EDUCATORI E FORMATORI DI SOGGETTI DEBOLI E VULNERABILI **16**

Percorsi progettati con l'obiettivo di diffondere una data security awareness e di fornire delle competenze tecniche di base che possano essere trasmesse ai discenti per favorire il loro inserimento nel mercato del lavoro.

LINEA DI ATTIVITÀ TRAIN THE TRAINERS RIVOLTA A DOCENTI DI STUDENTI K0-K8

Ciclo di incontri a beneficio di insegnanti di scuola primaria e secondaria di primo grado sulle competenze chiave e strategiche necessarie per rafforzare la consapevolezza ed i rischi in rete. Il percorso ha l'obiettivo di far evolvere e consolidare le conoscenze sui temi della cybersecurity ed il rischio informatico offrendo strumenti e metodologie utili per poterle trasferire agli studenti.

STRUTTURA DEL CORSO

- **80 ore complessive** di apprendimento (Webinar + Tutoraggio+ Laboratori + Materiali in self-study)
- **Webinar live: 4 moduli e 15 lezioni interattive**
- **Lezioni in e-learning** accessibili tramite piattaforma: scegli tu quando seguirle!
- **Massima flessibilità di partecipazione:** scegli tu quanti/quali moduli seguire e quando.
  Per una maggiore efficacia del percorso formativo, si consiglia la **frequenza ai moduli 1-2 per accedere ai moduli 3-4**
- **Rilascio digital Open Badge** con tecnologia *blockchain*

QUANDO

10 edizioni in partenza da **lunedì 15 settembre**

Scegli quella più comoda per te!

PER INFORMAZIONI:

PER ISCRIZIONI:

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

INDICE

modulo 01

INTRODUZIONE AL DIGITALE PER LA CYBERSICUREZZA (CBD)

articolazione del corso

ID 01 WEBINAR

2 ORE

- Introduzione al corso

ID 02 ALFABETIZZAZIONE DIGITALE PER EDUCATORI (ASINCRONO)

2 ORE

- Definizione e importanza della competenza digitale nel contesto educativo
- Il framework DigComp 2.2 e le competenze digitali per i docenti
- Panoramica delle tecnologie digitali nella didattica
- Digital divide e inclusione digitale
- L'evoluzione del ruolo del docente nell'era digitale

ID 03 ECOSISTEMA DIGITALE E CITTADINANZA DIGITALE (ASINCRONO)

2 ORE

- Comprensione dell'ecosistema digitale: internet, cloud, dispositivi connessi
- Concetti base di reti, dati e algoritmi
- Cittadinanza digitale: diritti e doveri nel mondo online
- Identità digitale e reputazione online
- Sostenibilità digitale e impatto ambientale delle tecnologie

ID 04 COMUNICAZIONE E COLLABORAZIONE DIGITALE (ASINCRONO)

3 ORE

- Strumenti di comunicazione digitale: email, chat, videoconferenze
- Piattaforme collaborative e condivisione di contenuti
- Netiquette e comunicazione efficace online
- Gestione dell'informazione digitale e organizzazione dei contenuti
- Introduzione ai concetti di privacy e protezione dei dati personali

ID 05 WEBINAR

2 ORE

- Conclusione del corso

modulo 02 INTRODUZIONE ALLA CYBERSICUREZZA (CBC)

articolazione del corso

ID 01 WEBINAR

2 ORE

- Introduzione al corso

ID 02 PROTEZIONE DEI DISPOSITIVI, DEI DATI ED EDUCAZIONE ALLA CYBERSICUREZZA

3 ORE

- Confidenzialità, Integrità e Disponibilità
- La catena della minaccia: debolezze, vulnerabilità, attacchi
- Tipologie di minacce: malware, virus, trojan, ransomware
- Vulnerabilità dei sistemi e dei dispositivi
- Finalità degli attacchi informatici più comuni
- Statistiche e casi reali di attacchi informatici nel settore educativo
- GDPR e normativa italiana sulla privacy
- Gestione dei dati personali degli studenti
- Consenso informato e diritti degli interessati

ID 03 INGEGNERIA SOCIALE

3 ORE

- Varie tipologie di attacchi tramite email di phishing e spam
- Sicurezza nella condivisione di documenti e allegati
- Cyber Hygiene
- Attacchi tramite altri mezzi
- Attacchi fisici
- Attacchi di tipo cognitivo
- Rischi e opportunità dei social network
- Impostazioni di privacy sui principali social media
- Cyberbullismo: riconoscimento, prevenzione e gestione
- Gestione dell'immagine digitale e reputazione online

ID 04 SICUREZZA NELLA NAVIGAZIONE WEB (ASINCRONO)

6 ORE

- Riconoscimento di siti web sicuri e non sicuri
- Gestione dei cookie e della privacy online
- Download sicuri e verifica dell'autenticità dei file
- Uso sicuro dei motori di ricerca e valutazione delle fonti

ID 05

CRITTOGRAFIA E PROTEZIONE DELLE INFORMAZIONI (ASINCRONO)

6 ORE

- Cos'è la crittografia: definizione semplice e scopo principale
- Differenza tra informazioni "in chiaro" e informazioni "cifrate"
- Concetti base di chiave di cifratura (senza entrare negli algoritmi complessi)
- Crittografia simmetrica vs asimmetrica spiegata con analogie semplici
- Funzioni di Hash e impronte digitali: cosa sono e a cosa servono
- Introduzione alla steganografia

ID 06

COME EDUCARE GLI STUDENTI ALLA CYBERSICUREZZA (ASINCRONO)

6 ORE

- Come insegnare la cybersicurezza in base all'età degli studenti
- Metodologie didattiche per la sicurezza digitale
- Risorse e materiali educativi disponibili
- Coinvolgimento delle famiglie nell'educazione digitale

ID 07

GESTIONE DEGLI INCIDENTI E PROCEDURE DI EMERGENZA (ASINCRONO)

6 ORE

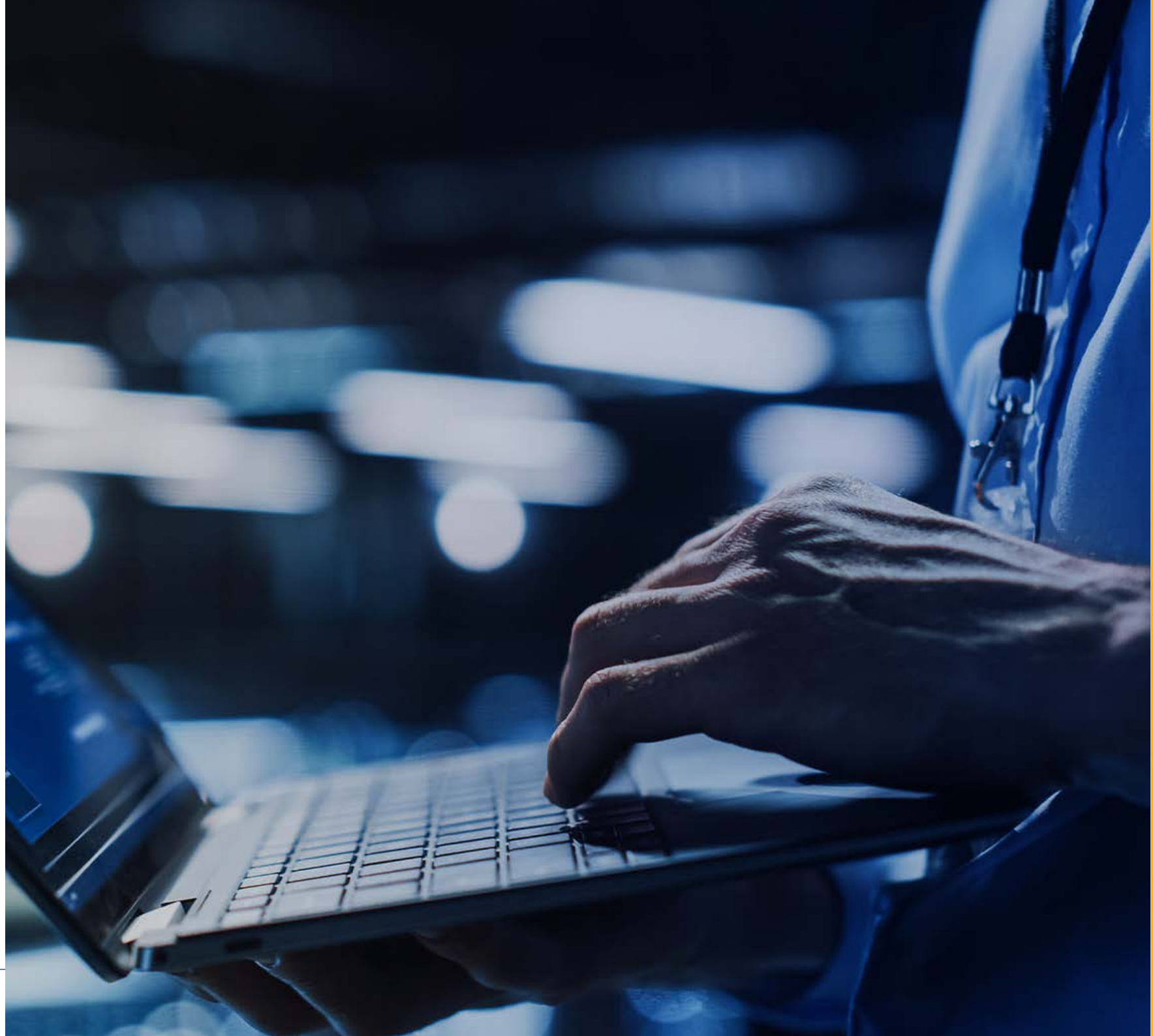
- Protocolli di risposta agli incidenti di sicurezza
- Segnalazione di comportamenti sospetti e attacchi
- Procedure di recupero in caso di compromissione
- Coordinamento con il referente per la sicurezza informatica dell'istituto

ID 08

ASPETTI LEGALI E RESPONSABILITÀ DEL DOCENTE (ASINCRONO)

7 ORE

- Quadro normativo sulla cybersicurezza nel settore educativo
- Responsabilità civili e penali legate alla sicurezza digitale
- Procedure disciplinari per violazioni della sicurezza
- Aggiornamento continuo e formazione permanente sulla cybersicurezza



modulo 03

INSEGNARE L'USO DI STRUMENTI PER LA PRIMARIA (CSP)

articolazione del corso

ID 01 WEBINAR

2 ORE

- Introduzione al corso

ID 02 PANORAMICA SU METODOLOGIE E STRUMENTI

2 ORE

- Escape room e didattica
- Vincoli normativi, come e quali strumenti usare?
- Metodologie didattiche ed escape room

ID 03 STRUMENTI DIGITALI (ASINCRONO)

18 ORE

- Presentazione “Pronto? Sig. Muschio!” (Luanti)
- Buone pratiche di “Pronto? Sig. Muschio!”
- Auctor
- Libreria H5P

ID 04 LABORATORIO

6 ORE

- Laboratorio in classe con supporto del tutoraggio in presenza o da remoto

ID 05 WEBINAR

2 ORE

- Conclusione del corso

modulo 04

CORSO PER INSEGNARE L'USO DI STRUMENTI PER LA SECONDARIA (CSS)

articolazione del corso

ID 01

WEBINAR

2 ORE

- Introduzione al corso

ID 02

PANORAMICA SU METODOLOGIE E STRUMENTI

2 ORE

- Escape room e didattica
- Vincoli normativi, come e quali strumenti usare?
- Metodologie didattiche ed escape room

ID 03

STRUMENTI DIGITALI (ASINCRONO)

18 ORE

- Nabbovaldo
- Libreria H5P

ID 04

LABORATORIO

6 ORE

- Laboratorio in classe con supporto del tutoraggio in presenza o da remoto

ID 05

WEBINAR

2 ORE

- Conclusione del corso

LINEA DI ATTIVITÀ TRAIN THE TRAINERS RIVOLTA A DOCENTI, EDUCATORI E FORMATORI DI SOGGETTI DEBOLI E VULNERABILI

Ciclo di incontri a beneficio di insegnanti, docenti, educatori, formatori, esperti ed operatori dell'apprendimento sulle competenze chiave e strategiche necessarie per rafforzare la consapevolezza ed i rischi in rete. È rivolto a insegnanti e docenti di scuole pubbliche e private di ogni ordine e grado o all'interno di ecosistemi protetti (CPIA o organizzazioni che trattano tutte le vulnerabilità).

obiettivo del corso

Il percorso ha l'obiettivo di far evolvere e consolidare le conoscenze sui temi della cybersecurity ed il rischio informatico offrendo strumenti e metodologie utili per poterle trasferire a soggetti con vulnerabilità e fragilità specifiche.

struttura

- **80 ore complessive** di apprendimento (Webinar degli incontri + Videolezioni + Materiali in self-study)
- **Webinar Incontri: 8 moduli di durata variabile da 1 a 3 ore**
- **Videolezioni+Self study:** approfondimenti dedicati ai contenuti tecnici della Cybersicurezza
- **Massima flessibilità di partecipazione:** scegli tu quanti/quali moduli seguire e quando.
- **Rilascio digital Open Badge** con tecnologia *blockchain*

QUANDO

10 edizioni in partenza a **luglio**

Date: **15, 16, 17, 18, 22 Luglio ore 14:30** o **ore 17:00**

Scegli quella più comoda per te!

INFORMAZIONI E ISCRIZIONI

Sito web: **https://serics.eu/tipologie/train-the-trainers**

Email: **academy@serics.eu**

articolazione del corso

modulo 01 — FAKE NEWS E IA

6 ORE

- Oltre il Digitale: Educare la Mente nell'Era dell'Iperconnessione (*Sincrona online)*
- Dalle fake news all'Intelligenza Arti-ficiale (*Sincrona online)*
- Dalle fake news all'Intelligenza Arti-ficiale (*Asincrona)*

modulo 02 — DIPENDENZA E DIG-ITALE

6 ORE

- Cervello in Rete: Cosa (ci) Fa il Digitale ai Processi Cognitivi ed Educativi (*Sincrona online)*
- Le dipendenze tecnologiche (*Sincrona online)*
- Riconoscere la dipendenza (*Asincrona)*

modulo 03 — L'AGGRESSIVITÀ ONLINE

8 ORE

- Connessioni Real(i): Recuperare Relazioni, Emozioni e Corpo nella Scuola Digitale (*Sincrona online)*
- L'aggressività e l'odio nella rete (*Sincrona online)*
- Strumenti (*Asincrona)*

modulo 04 — STRUMENTI DIGITALI PER L'INCLUSIVITÀ E L'APPRENDIMENTO

8 ORE

- Dall'iPhone al Cuore: Videogiochi, Dipendenze e Senso Critico tra Gioco e Cultura (*Sincrona online)*
- Strumenti digitali per l'inclusività e l'apprendimento (*Sincrona online)*
- Strumenti digitali per l'inclusività e l'apprendimento (*Asincrona)*

modulo 05 — BENESSERE DIGI-TALE: SPAZIO DI RI-FLESSIONE

4 ORE

- Presidiare il Cambiamento: Strategie Didattiche e Relazionali per un Digitale Educante (*Sincrona online)*
- Benessere digitale e spazio di riflessione (*Sincrona online)*

modulo 06

STRATEGIE EDUCA-TIVE PER LAVORARE IN CLASSE SULLA CONSAPEVOLEZZA DIGITALE

8 ORE

- Creazione di curricola sulla consapevolezza ed autonomia di competenze per navigare (*Sincrona online)*
- Tutela dei rischi e sicurezza in rete per gli studenti con difficoltà (*Sincrona online)*
- Il ruolo della scuola (*Asincrona - Caso Studio)*
- Le metodologie per una didattica digitale (*Asincrona - Esercitazione)*

modulo 07

SICUREZZA INFOR-MATICA E PROTE-ZIONE

12 ORE

- Consenso informato, trattamento dei dati personali e profilazione online (*Sincrona online)*
- Compliance normativa (*Asincrona)*
- Profilazione online (*Asincrona - Esercitazione)*
- Responsabilità civili e penali dei minori (*Sincrona online)*
- Approfondimento tematico (*Asincrona)*
- Gestire i dati (*Asincrona - Esercitazione)*
- Quiz autovalutativo (*Asincrona)*

modulo 08

CULTURA E CONSA-PEVOLEZZA NEL MONDO DIGITALE

29 ORE

- Disinformazione e fake news (*Sincrona online)*
- Sicurezza nell'uso dei dispositivi elettronici: Best-practice e misure di protezione dalle minacce in rete (*Sincrona online)*
- Percezione distorta del rischio cyber: riconoscere minacce non immediatamente visibili o riconoscibili (phishing, social engineering, profili falsi) (*Sincrona online)*
- Il panorama delle minacce (*Asincrona)*
- Strategie di sicurezza (*Asincrona)*
- Strategie difensive (*Asincrona)*
- Il mondo digitale (*Asincrona)*
- "Sai davvero cosa firmi?" (*Asincrona - Gaming)*
- Deepfake (*Asincrona - Gaming)*
- Laboratorio password (*Asincrona - Gaming)*
- Vulnerabilità (*Asincrona - Gaming)*
- Social engineering (*Asincrona - Gaming)*
- Profili falsi (*Asincrona - Gaming)*
- Simulazione Phishing (*Asincrona)*
- Approfondimento tematico (*Asincrona)*
- Quiz autovalutativo (*Asincrona)*

serics.eu/academy

academy@serics.eu

serics.eu

Finanziato dall'Unione europea NextGenerationEU

Ministero dell'Università e della Ricerca

Italiadomani
PIANO NAZIONALE DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE