FUTURA LA SCUOLA PER L'ITALIA DI DOMANI
Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Istruzione e del Merito
Italiadomani
Istituto Istruzione Superiore Statale
"S. Caterina da Siena-Amendola"
Scuola Capofila e Polo di Formazione Ambito SA-23
Settori: Economico – Tecnologico – Enogastronomia e Ospitalità Alberghiera
Via Lazzarelli – 84132 Salerno Tel. 089333084 – C.F. 95139760656 – CM: SAIS06900N – CU: UFS8JP
PEO: sais06900n@istruzione.it PEC: sais06900n@pec.istruzione.it – Sito Web: www.santacaterina-amendola.edu.it

Atti/Sito web

Progetto "Formazione transizione digitale del personale scolastico, CUP F54D23003050006, codice identificativo progetto: M4C112a1-2023-1222-P-33073 finanziato nell'ambito del decreto. n. 66 del 12/04/2023 del Ministro dell'istruzione, Missione 4 Istruzione e Ricerca — Componente 1 – Potenziamento dell'offerta dei servizi di istruzione: dagli asili nido alle Università — Investimento 2.1: Didattica digitale integrata e formazione alla transizione digitale per il personale scolastico"

Metodologie didattiche innovative per l'insegnamento e l' apprendimento connesse con l'utilizzo delle nuove tecnologie

Il progetto si propone si propone di raggiungere le seguenti finalità

- Migliorare la consapevolezza di una cultura della sicurezza attraverso l'utilizzo di strumenti tecnologici che sono comunemente usati in tutte le nostre attività giornaliere, siano essere legate al lavoro o al normale essere di cittadini.
- Favorire lo sviluppo di competenze digitali: il partecipante sarà in grado di effettuare le attività di Vulnerability Assessment di una Infrastruttura Critica valutandone i risultati ottenuti al fine di suggerire agli stakeholder le giuste attività da intraprendere per ridurre i rischi che la minacciano.
- Offrire agli studenti risorse didattiche innovative per poter calare i principi fondamentali della Data Security ai contesti di networking più recenti (Cloud Computing, Edge Computing, Fog Computing, IoT) riuscendo a valutare ed arginare i rischi a cui tali contesti sono attualmente soggetti facendo predisporre adeguate contromisure
- I partecipanti devono dimostrare di saper applicare metodi e strumenti per la rilevazione dei rischi e per la protezione dei sistemi software a determinati contesti d'uso o ambienti operativi.

PROGRAMMA

Introduzione alle problematiche relative alla cybersecurity e alle metodologie didattiche innovative che tengano conto delle attuali e future minacce verso i diversi sistemi informatici disponibili, ovvero cloud, datacenter, workstation, PC, dispositivi mobili e IOT. Verranno illustrati i concetti base che stanno dietro a quella che è la triade della sicurezza, la famosa CIA (Confidenzialità, Integrità, Disponibilità). Ingegnerizzazione e progettazione di un sistema sicuro in ambito multipiattaforma per la gestione di gruppi di lavoro in un contesto collaborativo.

Il partecipante acquisirà padronanza con i principali temi di Network Security, tra cui firewalling, anomaly detection, steganography, honeypot, social engineering.

Calendario incontri

10/01/2025	VENERDI	4
17/01/2025	VENERDI	4
23/01/2025	GIOVEDI	4
27/01/2025	LUNEDI	4
10/02/2025	LUNEDI	3
12/02/2025	MERCOLEDI	4
17/02/2025	LUNEDI	4
21/02/2025	VENERDI	3

*Eventuali modifiche degli incontri saranno tempestivamente comunicate.

Il Dirigente Scolastico
Prof.ssa Anna Rita Carrafiello
ANNA RITA CARRAFIELLO
12.12.2024 12:07:01 UTC

**Documento informatico firmato digitalmente ai sensi del D.Lgs. 82/2005 s.m.i e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa*