WEBINAR

SICUREZZA INFORMATICA E NORMATIVE PER SISTEMI CRITICI

Allo scopo di lavorare in maniera congiunta con il mondo accademico e definire dei progetti di formazione strutturati che possano garantire opportunità a tutte le aziende associate, è stato costituito un accordo di collaborazione tra ANIE ASSIFER e CINI (Consorzio Interuniversitario Nazionale per l'Informatica), principale punto di riferimento della ricerca accademica nazionale nei settori dell'Informatica e dell'Information Technology.
Il progetto di collaborazione prevede dei percorsi di formazione sulle nuove tecnologie in ambito ferroviario suddivisi in quattro aree tematiche (Computer Architectures, Design Methodologies, Machine Learning e Programming & Simulations).

Obiettivi

Il corso di cybersecurity per sistemi critici offre ai partecipanti competenze avanzate sulla sicurezza e la conformità normativa. Il corso si propone di introdurre i controlli di sicurezza secondo gli standard NIST e del FNCS, le metodologie di Business Impact Analysis (BIA) e le tecniche per l'analisi dei rischi connessi alla sicurezza informatica. La formazione prosegue con un focus su hardware security, affrontando side-channel attack e protocolli per gestione delle informazioni sensibili, come le chiavi di sicurezza. La parte finale è dedicata alla safety del software con riferimento alle normative EN50128 e alla nuova EN50716 per un quadro completo sulla sicurezza dei sistemi critici.

Relatori

Prof. Mario Barbareschi - Prof.ssa Valentina Casola

Università degli Studi di Napoli Federico II

Calendario

LEZIONE	DATA	ORARIO	ORE
1	9 Settembre 2025	9:00 – 13:00	4
2	16 Settembre 2025	9:00 – 13:00	4
3	17 Settembre 2025	9:00 – 13:00	4
4	23 Settembre 2025	9:00 – 13:00	4
5	25 Settembre 2025	9:00 – 13:00	4
6	30 Settembre 2025	9:00 – 13:00	4
7	2 Ottobre 2025	9:00 – 13:00	4
8	7 Ottobre 2025	9:00 – 13:00	4
9	9 Ottobre 2025	9:00 – 13:00	4
10	14 Ottobre 2025	9:00 – 13:00	4
		TOTALE ORE	**40**

Modalità e quota di iscrizione

1. Quota di partecipazione: Associato ANIE € 350,00+IVA
2. Pagamento: con carta di credito o con bonifico bancario.

   Per pagamento con bonifico bancario inviare copia del pagamento a formazione@anieservizintegrati.it e amministrazione@anieservizintegrati.it

   In mancanza dell'invio della distinta di pagamento, l'iscrizione non si perfeziona.
3. Successivamente saranno inviate le modalità di partecipazione al webinar.

Programma

Lezione 1

- Introduzione alla cybersecurity
- proprietà di sicurezza
- il concetto di minaccia, vulnerabilità e controllo
- threat intelligence
- risorse disponibili per l'identificazione e classificazione delle minacce, vulnerabilità e attacchi (threat taxonomies, Mitre CVE/CWE, Mitre Att&ck Frameworkm Mitre CAPEC)
- Laboratorio di threat modeling: STRIDE e il Microsoft Threat Modeling Tool

Lezione 2

- Analisi del rischio di sicurezza
- il concetto di rischio e i fattori associati al rischio
- il processo di gestione del rischio
- metodi qualitativi e quantitativi per la stima del rischio
- Laboratorio di risk analysis: OWASP Risk Rating Methodology
- Approcci standard alla gestione del rischio di sicurezza
- NIST Risk Management Framework
- NIST Cybesecurity Framework
- Framework Nazionale per la Cybesecurity e la Data Protection

Lezione 3

- Elementi di Crittografia applicata
- Crittografia Simmetrica
- Crittografia Asimmetrica

Lezione 4

- Controlli di sicurezza per l'Identity and Access Control alla luce del nuovo regolamento EIDAS 2
- Controlli di sicurezza per la protezione delle reti di comunicazione

Lezione 5

- Normativa italiana ed Europea in tema di cybersecurity
- Direttiva NIS2
- Perimetro Nazionale di Sicurezza Cibernetica

Lezione 6

- Hardware Security and Trust
- Supply chain
- Normative per Hardware Security
- Secure enclave

Lezione 7

- Side channel attacks
- Simple power analysis
- Differential Power Analysis
- Attacchi distruttivi e fault injection
- Contromisure e tecniche difensive

Lezione 8

- Introduzione al Trusted computing
- Tecnologie per il Digital Right Management
- Soluzioni commerciali e standard per il trusted computing

Lezione 9

- Tecnologie di Trusted Computing
- Trusted Platform Module
- funzioni principali del TPM
- ARM TrustZone
- Intel SGX

Lezione 10

- Safety e Security: Normativa EN50128
- Gestione dei requisiti
- Gestione dei test
- Sicurezza delle comunicazioni: EN50156