SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

SERICS CYBERSECURITY ACADEMY

2025

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

INDICE
DEI CONTENUTI

01.
FONDAZIONE SERICS

La Fondazione SERICS (**Se**curity and **Ri**ghts in the **C**yber**S**pace) promuove l'innovazione e la ricerca nel campo della sicurezza informatica e della protezione dei diritti digitali. È una partnership pubblico-privata che coinvolge 23 realtà tra università statali (11), centri di ricerca (7) e aziende leader (5). I progetti di ricerca sono coordinati da 10 spoke, strutture accademiche dedicate ciascuna un'area tematica strategica per la cybersecurity distribuite su tutto il territorio nazionale. Il partenariato opera su scala nazionale come soggetto attuatore del programma "Cybersecurity, nuove tecnologie e tutela dei diritti", previsto nell'ambito del PNRR - Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e Ricerca" per realizzare 27 progetti di ricerca di cybersecurity con l'ambizione di contribuire alla difesa dello spazio cibernetico a livello planetario.

PARTNER

UniSA – Università degli Studi di Salerno (HUB)
CNIT – Consorzio Nazionale Interuniversitario per le Telecomunicazioni
PoliTO – Politecnico di Torino (Spoke 7)
FBK – Fondazione Bruno Kessler
UniBO – Alma Mater Studiorum – Università di Bologna (Spoke 7)
UniCA – Università degli Studi di Cagliari (Spoke 3)
UniCAL – Università della Calabria (Spoke 5)
UniFI – Università degli Studi di Firenze
UniGE – Università degli Studi di Genova (Spoke 4)
UniMI – Università degli Studi di Milano (Spoke 10)
UniRoma1 – Sapienza Università di Roma (Spoke 9)
UniVE – Università Ca' Foscari Venezia (Spoke 6)

CINI – Consorzio Interuniversitario Nazionale per l'Informatica
CNR – Consiglio Nazionale delle Ricerche
UniBA – Università degli Studi di Bari Aldo Moro
IMT – Scuola IMT Alti Studi Lucca
FUB – Fondazione Ugo Bordoni
SSSA – Scuola Superiore Sant'Anna di Pisa

ENI
FINCANTIERI
ISP – Intesa Sanpaolo SpA
Leonardo S.p.A.
Telsy S.p.A.

02.
SERICS CYBERSECURITY ACADEMY

La SERICS Cybersecurity Academy è il programma formativo della Fondazione SERICS nato per rafforzare le competenze italiane ed europee in ambito cybersecurity, sovranità digitale e protezione dei dati e ha il compito di curare, organizzare ed erogare attività formative rivolte a studenti, docenti, formatori, dipendenti e altri da realizzarsi mediante conferenze, seminari, piattaforme di formazione, cyber-game personalizzate. L'offerta formativa di eccellenza è erogata da docenti provenienti dal mondo accademico ed esperti di settore.

COMITATO SCIENTIFICO

Prof. Alessandro ARMANDO, Università degli Studi di Genova - Presidente

Prof. Francesco BUCCAFURRI, l'Università della Calabria
Prof. Danilo CAIVANO, l'Università degli studi di Bari "Aldo Moro"
Prof. Michele COLAJANNI, l'Università degli studi di Bologna "Alma Mater Studiorum"
Prof. Stefano DI CARLO, il Politecnico di Torino
Prof. Giuseppe FENZA, l'Università degli studi di Salerno
Prof. Riccardo FOCARDI, l'Università degli studi di Venezia "Cà Foscari"
Prof. Giorgio GIACINTO, l'Università degli studi di Cagliari
Prof. Leonardo QUERZONI, l'Università degli studi di Roma "La Sapienza"
Prof.ssa Pierangela SAMARATI, l'Università degli studi di Milano
Prof. Andrea SIMONCINI, l'Università degli studi di Firenze

Prof. Giuseppe BIANCHI, Consorzio interuniversitario per le Telecomunicazioni CNIT
Prof. Alessandro BIONDI, Scuola Superiore di Studi Universitari e di Perfezionamento Sant'Anna di Pisa
Prof. Gabriele COSTA, Scuola IMT Alti Studi Lucca
Prof.ssa Elena FERRARI, Consorzio interuniversitario per l'informatica CINI
Dr. Fabio MARTINELLI, Centro Nazionale delle Ricerche C.N.R.
Prof. Silvio RANISE, Fondazione Bruno Kessler
Dr.ssa Marina SETTEMBRE, Fondazione Ugo Bordoni

03.
MISSION, OBIETTIVI E TARGET

MISSION

Promuovere una cultura della sicurezza informatica che coniughi:

- Eccellenza tecnologica
- Consapevolezza normativa
- Tutela dei diritti digitali

OBIETTIVI

Rafforzare, integrare e creare nuove competenze per migliorare la sicurezza degli asset tecnologici formando professionisti, ricercatori e decisori pubblici capaci di progettare, gestire e difendere infrastrutture, sistemi e dati complessi in un'ottica di resilienza.

Diffusione e condivisione di conoscenze ed *expertise* attraverso l'utilizzo di sistemi e tecniche di difesa del cyberspazio allo stato dell'arte.

TARGET

- Professionisti e dipendenti pubblici/privati
- Aziende e pubbliche amministrazioni che vogliono aggiornare o potenziare le competenze interne
- Studenti neo-laureati e dottorandi
- Insegnanti e formatori (in ottica "Train the Trainers")

Le sessioni di formazione si terrano nel periodo aprile – dicembre 2025

03.
OFFERTA FORMATIVA

1

FORMAZIONE
SPECIALISTICA
PER DIPENDENTI
E PROFESSIONISTI

2

PROMOZIONE
E SUPPORTO
DI SCUOLE
SPECIALISTICHE
DI DOTTORATO

3

PROMOZIONE
E SUPPORTO
DI MASTER
UNIVERSITARI

4

CORSO DI
IMPRENDITORIALITÀ
PER LAUREANDI,
NEO-LAUREATI,
DOTTORANDI E
NEO-DOTTORATI

5

TRAIN THE
TRAINERS – SOGGETTI
VULNERABILI

1

FORMAZIONE SPECIALISTICA PER DIPENDENTI E PROFESSIONISTI

Cyber Threats & Defense

Difesa dagli attacchi avanzati, offuscati e evasivi

Penetration Test e Intrusion Detection

Hardening di sistemi e servizi Linux

Collezionamento, l'analisi e la correlazione degli eventi

Contrastare la disinformazione: Strumenti e Tecniche per la gestione delle Minacce e dei Rischi

Software & System Security

Sicurezza del software: prevenzione delle vulnerabilità tramite programmazione sicura

Intelligenza Artificiale: progettazione sicura e robusta

Sicurezza e privacy nei dispositivi mobili

Aspetti di sicurezza nei dispositivi embedded

Aspetti di sicurezza e relative normative nel mondo automotive

Data Protection & Privacy

La sicurezza dei dati e dei servizi nella trasformazione digitale

Privacy e sicurezza nella condivisione e gestione dei dati in scenari emergenti

Digital Sovereignty: Beyond tensions of data protection and cybersecurity

Cryptography & Authentication

Crittografia e applicazioni

Protocolli e tecnologie per l'autenticazione, l'identità e la firma digitale

Risk Management & Evaluation Frameworks

Common Criteria for Information Technology Security Evaluation

Framework e Standard open per Cyber Risk Assessment

Framework e Standard commerciali per Cyber Risk Assessment

Security of Cloud & Emerging Technologies

Orchestratori distribuiti e applicazioni "Cloud Native"

2

PROMOZIONE E SUPPORTO DI SCUOLE SPECIALISTICHE DI DOTTORATO

Il percorso formativo fornisce formazione specialistica ed integrativa in corsi di dottorato di ricerca beneficiari.

Le attività formative prevedono l'istituzione 10 scuole specialistiche, ciascuna specializzata in una specifica area tematica degli spoke previsti.

Le principali aree tematiche riguardano gli ambiti della sicurezza dei sistemi informativi e loro virtualizzazione, la sicurezza delle infrastrutture tecnologiche e del software, tematiche di *data protection* nonché tutti gli aspetti legati alla disinformazione agli aspetti umani, sociali e legali.

Obiettivi e risultati attesi:

- Contribuire alla formazione di una nuova generazione di ricercatori specializzati sulla Cybersecurity e sulla tutela dei Diritti del Cyber Space
- Promuovere la contaminazione dei saperi tra gli aspetti tecnologici, giuridici e sociopolitici in tema di Cybersecurity

3

PROMOZIONE E SUPPORTO DI MASTER UNIVERSITARI

Le attività riguardano la **promozione** e il **supporto di master universitari** sulle tematiche ambito del mandato della Fondazione SERICS.

- Metodi di rilevamento delle minacce
- Privacy Enhancing Technologies (Pet)
- Difesa Perimetrale

Obiettivi e risultati attesi:

- Analizzare metodi di rilevamento di minacce informatiche
- Migliorare la capacità di rilevare minacce in tempo reale
- Analizzare *best practice* per la gestione degli incidenti
- Approfondire varietà di soluzioni e approcci tecnologici delle PET
- Configurare e gestire un *firewall*
- Analizzare funzionalità avanzate dei *firewall*
- Approfondire metodologie di indagine digitale
- Approfondire l'approccio della *Zero Trust Architecture*

4

CORSO DI IMPRENDITORIALITÀ PER LAUREANDI, NEO LAUREATI, DOTTORANDI E NEO DOTTORATI

Il corso, erogato in modalità blended, ha l'obiettivo di **fornire ai partecipanti una comprensione completa del processo imprenditoriale**, dalla definizione della vision e della strategia alla gestione delle risorse e dei rischi, con particolare attenzione all'integrazione delle tecnologie digitali e della sicurezza informatica nella governance aziendale.

- SCENARI MACROECONOMICI E CHANGE MANAGEMENT
- MINDSET IMPRENDITORIALE E GESTIONE DEL RISCHIO
- BUSINESS PLANNING E SOSTENIBILITÀ FINANZIARIA
- PROBLEM SOLVING E DECISION MAKING
- SOSTENIBILITÀ D'IMPRESA E ESG STRATEGY
- INNOVAZIONE, DIGITALIZZAZIONE E CYBERSECURITY NELLA GESTIONE D'IMPRESA
- LEADERSHIP, COMUNICAZIONE E TEAM MANAGEMENT
- MARKETING, BRANDING E POSIZIONAMENTO STRATEGICO
- FINANZA D'IMPRESA DI BASE
- DIRITTO D'IMPRESA E REGOLAMENTAZIONE INTERNAZIONALE
- OPERATIONS & SUPPLY CHAIN MANAGEMENT
- STRATEGIE PER L'INTERNAZIONALIZZAZIONE E LEAN MANAGEMENT
- HR E RELAZIONI INDUSTRIALI
- "CYBERMONOPOLY" - BUSINESS GAME SULLA GESTIONE D'IMPRESA E CYBERSECURITY
- BUSINESS GAME "CYBER SHARK TANK" - CYBERSECURITY EDITION

Obiettivi e risultati attesi:

- Acquisire competenze orientate all'imprenditorialità
- Saper realizzare un business plan in funzione della creazione d'impresa
- Conoscere e saper applicare tecniche e strumenti di conduzione di un'impresa

5

TRAIN THE TRAINERS – SOGGETTI VULNERABILI

Il corso per i formatori ha 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 percorso, i formatori saranno, quindi, in grado di:

- Identificare le esigenze di sensibilizzazione e istruzione in materia di cybersecurity, dunque individuare le caratteristiche specifiche del target
- Progettare e sviluppare dei programmi di apprendimento connessi alle esigenze riscontrate e al target
- Sviluppare esercitazioni di cybersecurity o utilizzare quelle che verranno fornite durante il percorso
- Erogare test di valutazione delle attività realizzate
- Identificare e selezionare approcci pedagogici appropriati per il pubblico cui si rivolgono

Train the trainers - Studenti K0-K8. I percorsi sono progettati con l'obiettivo primario di creare consapevolezza in merito alle criticità dovute a una scarsa attenzione alla gestione dei dati.

Train the trainers – Soggetti vulnerabili
I percorsi sono 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.

05.

COSTRUIAMO L'OFFERTA FORMATIVA INSIEME

La SERICS Cybersecurity Academy costruisce insieme al Committente, partendo dai suoi fabbisogni, il percorso più idoneo e funzionale sia in termini di organizzazione che di contenuti didattici.

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