FONDAZIONE BRUNO KESSLER
MAGAZINE

# Un framework condiviso per la sicurezza del cloud europeo

20 Marzo 2026

## Nell’iniziativa 8ra, FBK contribuisce allo sviluppo del Collaborative Security Framework per l’ecosistema IPCEI-CIS

Garantire sicurezza, interoperabilità e fiducia nelle infrastrutture digitali europee è una delle sfide chiave nello sviluppo del **Cloud-Edge Continuum**, l’ecosistema tecnologico su cui si baseranno molti dei servizi digitali del futuro. In questo contesto nasce il **Collaborative Security Framework (CSF)**, un documento strategico sviluppato nell’ambito del **Cross Workstream on Security dell’iniziativa 8ra**, che definisce le policy di sicurezza per l’intero ecosistema **IPCEI-CIS**.

Alla sua realizzazione ha contribuito anche la **Fondazione Bruno Kessler**, attraverso le attività del Centro per la Cybersecurity, impegnato nello sviluppo di soluzioni avanzate per la protezione delle infrastrutture digitali europee.

Il CSF ha l’obiettivo di stabilire una base comune per proteggere i diversi *building block* che compongono l’architettura di riferimento dell’iniziativa. Attraverso un approccio strutturato e collaborativo, il framework consente di identificare, classificare e integrare i componenti di sicurezza sviluppati nei diversi progetti, garantendo al tempo stesso interoperabilità e conformità a standard condivisi.

### Un framework collaborativo per la sicurezza

All’interno dell’ecosistema 8ra, ciascun progetto contribuisce allo sviluppo di almeno un componente infrastrutturale. Il **Collaborative Security Framework** ha l’obiettivo di definire i principi fondanti per la sicurezza di questi building block, garantire la loro conformità rispetto al framework stesso e organizzare le loro interfacce permettendone l’interoperabilità. L’idea è di classificare i diversi componenti in base alla loro funzione e al livello architetturale in cui operano, facilitando l’integrazione tra le soluzioni e promuovendo l’adozione di un linguaggio comune per la sicurezza.

Questo modello consente inoltre di individuare eventuali sovrapposizioni tra componenti simili e, allo stesso tempo, di evidenziare possibili lacune nell'architettura di sicurezza complessiva, favorendo lo sviluppo di nuovi elementi essenziali per rafforzare l'ecosistema.

Il framework introduce anche un percorso iterativo articolato in dieci fasi che guida i partner verso livelli sempre più elevati di maturità della sicurezza. Il processo parte dall'identificazione e classificazione dei componenti sviluppati nei progetti IPCEI-CIS. Prosegue poi con l'analisi delle differenze tra soluzioni analoghe, la raccolta delle informazioni tecniche e funzionali e l'individuazione di eventuali elementi mancanti. A queste attività si affiancano la definizione di una baseline di conformità, la valutazione dei componenti nei diversi pilot dell'iniziativa e l'aggiornamento continuo del framework per rispondere all'evoluzione dei requisiti tecnologici e delle minacce informatiche.

## Il contributo di FBK

Il lavoro di definizione del framework ha coinvolto diversi partner dell'ecosistema 8ra impegnati nel Cross Workstream on Security. Tra questi anche la Fondazione Bruno Kessler, che attraverso il Centro per la Cybersecurity contribuisce allo sviluppo di soluzioni avanzate per la protezione delle infrastrutture digitali europee. Per FBK ha partecipato ai lavori il ricercatore **Salvatore Manfredi**, autore e curatore del documento. Nel corso delle attività ha coordinato il **Topic 3 "Data Security"**, facilitando il confronto tra le diverse aziende partner coinvolte nel progetto e contribuendo alla definizione delle linee guida per l'integrazione dei componenti di sicurezza. Ha inoltre lavorato alla definizione della struttura del framework e alla stesura delle parti dedicate all'integrazione dei componenti di sicurezza, individuando gli elementi tecnici necessari per rendere il modello applicabile all'interno dell'ecosistema IPCEI-CIS.

Questo lavoro si inserisce nell'impegno più ampio della Fondazione Bruno Kessler nello sviluppo non solo di soluzioni tecnologiche per la cybersecurity e per le infrastrutture digitali europee ma anche di individuare best practice che a livello metodologico da una parte rendano più efficace l'integrazione delle soluzioni tecnologiche e allo stesso tempo contribuiscano a creare una cultura della sicurezza diffusa tra tutti i profili professionali che lavorano in ambito IT che, pur essendo esperti in vari aspetti di dominio mancano spesso di una specifica formazione rispetto ai rischi di cybersecurity.  Il miglioramento di una postura di sicurezza sia dal punto di vista tecnico che organizzativo e' fondamentale per la costruzione di ecosistemi complessi come quelli sviluppati nel progetto IPCEI-CIS contribuendo alla loro resilienza, interoperabilità e affidabilità.  Questo e' un passo decisivo per costruire un'alternativa Europea alle infrastrutture digitali americane e asiatiche e aumentare la sovranità tecnologica Europea come indicato anche dal punto di vista legale con le Direttive NIS2 (Network Infrastructure Security) per le infrastrutture critiche e DORA (Digital Operational Resilience Act) per le banche e i servizi finanziari.

In questo contesto, il **Collaborative Security Framework** rappresenta un contributo importante sia alla realizzazione del Single Digital Market che di un maggiore autonomia digitale in un contesto geopolitico che richiede una sempre maggiore attenzione alla gestione dei rischi di cybersecurity sia in tempo di pace che, purtroppo, di guerra.

**LINK**

https://magazine.fbk.eu/it/news/un-framework-condiviso-per-la-sicurezza-del-cloud-europeo/

**TAG**

- #8ra
- #building block
- #CFS
- #Cloud-Edge Continuum
- #cybersicurezza
- #framework
- #infrastrutture digitali
- #IPCEI-CIS
- #IPCEICIS
- #sicurezza

**MEDIA COLLEGATI**

- 8ra Initiative: https://www.8ra.com/
- 8ra Collaborative Security Framework (CSF): https://www.8ra.com/news/establishing-a-unified-security-architecture-the-8ra-collaborative-security-framework-csf/

**AUTORI**

- Michela Antino