GARR NEWS

il magazine della rete dell'università e della ricerca

ISSN 2039-8271

numero 33 | 2025

garrnews.it

Reti e data centre
Nuove strategie per un'evoluzione sostenibile

Sicurezza informatica
Un approccio collaborativo per difendersi al meglio

Servizi di rete
Certificati digitali, DNS, eduVPN: ecco le novità

Scienza aperta
Il ruolo chiave dell'Italia in ambito internazionale

Chi siamo

Siamo la rete nazionale ad altissima velocità dedicata alla comunità dell'istruzione, della ricerca e della cultura in Italia. La rete GARR è ideata e gestita dal Consortium GARR, associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Università e della Ricerca.
Gli enti soci sono CNR, ENEA, Fondazione CRUI, INAF, INFN, INGV, le università statali italiane, gli Istituti di Ricovero e Cura a Carattere Scientifico (IRCCS) e gli Istituti Zooprofilattici Sperimentali (IZS).

Mission

Fin dagli albori di Internet, il nostro principale obiettivo è fornire connettività ad alte prestazioni e sviluppare servizi innovativi per le attività quotidiane di docenti, ricercatori e studenti e per la collaborazione a livello internazionale.

Valori

Collaborazione e inclusività sono i nostri valori fondanti.
Al centro della strategia ci sono le esigenze della nostra comunità alla quale garantiamo connessioni e servizi neutrali, trasparenti, semplici e affidabili.

Il filo

Claudia Battista
Direttrice
GARR

Care lettrici, cari lettori,

la parola che attraversa questo numero è **sostenibilità**, intesa nel suo significato più ampio: ambientale, tecnologico, economico e sociale. Non come obiettivo astratto, ma come criterio guida per progettare infrastrutture digitali capaci di durare nel tempo, adattarsi al cambiamento e continuare a generare valore per la comunità della ricerca e dell'istruzione.

La sostenibilità passa innanzitutto dal modo in cui progettiamo e gestiamo le infrastrutture fisiche. I **data centre**, cuore pulsante della trasformazione digitale, sono chiamati a conciliare potenza di calcolo e responsabilità ambientale. L'evoluzione verso modelli basati su osservabilità avanzata, AI e gestione predittiva dell'energia indica una direzione di sviluppo lungo la quale è possibile migliorare l'efficienza complessiva e ridurre consumi ed emissioni, mantenendo alti livelli di prestazioni e affidabilità. Un percorso progressivo che punta a rendere il data centre un ecosistema sempre più intelligente e sostenibile.

In questa direzione si colloca anche l'**automazione della rete** GARR con PACMAN, che racconta un cambiamento culturale prima ancora che tecnologico: processi condivisi, modelli ripetibili e una gestione più affidabile di infrastrutture sempre più complesse.

Nella stessa prospettiva si inseriscono gli investimenti del **PNRR**, con i progetti TeRABIT e ICSC, che hanno contribuito a costruire un'infrastruttura nazionale integrata di rete, calcolo e dati, riducendo i divari territoriali e creando le condizioni perché le infrastrutture realizzate oggi restino utili e scalabili anche domani.

Sostenibilità significa anche resilienza. La **sicurezza** diventa un pilastro della trasformazione digitale e i Security Days e i gruppi di lavoro GARR mostrano come la risposta più efficace alle minacce informatiche sia collettiva, basata su formazione, strumenti comuni e condivisione delle esperienze.

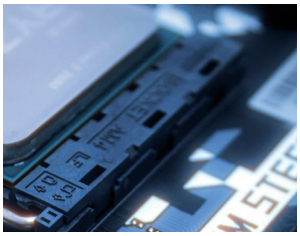
La sostenibilità passa inoltre attraverso servizi capaci di garantire un accesso equo e affidabile alle risorse digitali. L'esperienza dell'Università Ca' Foscari con **eduVPN** dimostra come sia possibile modernizzare l'accesso remoto migliorando sicurezza e usabilità, riducendo costi e barriere per gli utenti.

Allargando lo sguardo, la sostenibilità assume una dimensione strategica europea. Le reti della ricerca rappresentano un pilastro spesso invisibile ma decisivo dell'**autonomia digitale** del continente.

In filigrana emerge un messaggio chiaro: **la sostenibilità non nasce da una singola tecnologia o da un singolo progetto, ma da scelte coerenti, collaborazione e capacità di tenere insieme innovazione e responsabilità**.
È questa visione che rende le infrastrutture digitali affidabili, condivise e capaci di durare nel tempo.

Buona lettura!

In questo numero



caffè scientifico

3
Come rendere sostenibili i data centre
di Elis Bertazzon

6
Data centre: la sostenibilità passa dall'acqua
di Marta Mieli

9
Innovare nell'età del cambiamento
di Elis Bertazzon

storie della comunità

12
Modernizzare l'accesso remoto in ambito accademico: la migrazione di Ca' Foscari a eduVPN
di Stefano Claut (Università Ca'Foscari Venezia)

14
Collaborare per la sicurezza: l'esperienza condivisa tra atenei
di Erika Trotto

servizi alla comunità

17
DNSSEC: un valido aiuto per la sicurezza
di Carlo Volpe

19
TCS GARR: un tool di automazione per i certificati digitali
di Carlo Volpe

networking

21
PACMAN: l'automazione che sta cambiando la rete GARR
di Erika Trotto

23
PNRR: il bilancio dei progetti TeRABIT e ICSC e il ruolo strategico di GARR
di Sara Di Giorgio

cybersecurity

26
Security Awareness Boost
di Simona Venuti

29
Dai Security Days ai gruppi di lavoro. Formazione NIS2 e collaborazione nella comunità GARR
di Marta Mieli, Alessandro Inzerilli e Leonardo Lanzi

internazionale

31
EOSC entra nella fase operativa
di Sara Di Giorgio

33
Skills4EOSC: l'ecosistema europeo delle competenze in open science
di Sara Di Giorgio

35
FP10: non è ancora finita
di Marco Falzetti (APRE)

37
Il pilastro invisibile dell'autonomia digitale in Europa
di Elis Bertazzon

protagonisti

39
Internet è di tutti. 25 anni di ISOC a difesa di un bene comune
di Stefano Giordano (ISOC)

le rubriche

1
Il filo

16
La ricerca comunica

41
Le sedi connesse alla rete GARR

48
I servizi GARR

Come rendere sostenibili i data centre

Osservabilità, AI generativa e gestione intelligente dell'energia. Dall'università, prospettive diverse e sinergiche verso un obiettivo comune.

di Elis Bertazzon

Con la crescita esponenziale della potenza di calcolo, alimentata dal cloud, dall'AI generativa e dalla continua espansione dei servizi digitali, la sostenibilità dei data centre più efficienti, resilienti e a basso impatto ambientale richiede la convergenza di competenze diverse: ICT, ingegneria energetica, modellazione e AI. Un tema quanto mai attuale in un momento storico in cui ridurre i consumi e le emissioni è una priorità globale.

Questo tema è stato al centro della sessione moderata da **Daniela Galetti,** responsabile dell'unità Gestione Sistemi, Storage e Reti HPC di Cineca dedicata alla sostenibilità nel corso del Workshop GARR 2025, che si è tenuto a Roma lo scorso novembre. Gli interventi di **Andrea Bartolini**, professore di ingegneria informatica dell'Università di Bologna e **Alfonso Capozzoli**, professore di fisica tecnica ambientale del Politecnico di Torino, hanno offerto una visione complementare ma coerente di questo percorso: dall'osservabilità avanzata alla gestione predittiva, fino alla possibilità, ormai concreta, di interagire con infrastrutture complesse usando il linguaggio naturale. Un dialogo che, come sottolineato da Galetti, ha evidenziato la convergenza di approcci diversi verso obiettivi comuni, producendo un confronto ricco e sinergico.

Dati al centro: dall'osservabilità all'autonomia

Andrea Bartolini ha ricostruito l'evoluzione dei sistemi di monitoraggio dei data centre negli ultimi 20 anni, mostrando come la sostenibilità passi sempre più dalla capacità di raccogliere, leggere e interpretare la telemetria in modo efficiente. Laddove un tempo la gestione dei dati avveniva in modo manuale e frammentato, l'avvento di IoT, Big Data e sistemi distribuiti ha permesso di acquisire informazioni da milioni di sensori e di metterle a disposizione attraverso pipeline scalabili e standardizzate. Un esempio in questa direzione è Examon, software open source sviluppato con CINECA e altri partner, che centralizza dati eterogenei relativi a hardware, software e facility, rendendoli immediatamente utilizzabili per analisi e simulazioni.

Questa disponibilità di informazioni ha reso possibile la costruzione di digital twin dell'infrastruttura, modelli attraverso cui gli operatori possono analizzare criticità, testare scenari o individuare rapidamente situazioni anomale. In un caso concreto citato da Bartolini, l'ottimizzazione dei sistemi di raffreddamento tramite dashboard intelligenti ha portato a una riduzione dell'8% dei consumi legati a questa componente, dimostrando l'impatto reale che un approccio integrato ai dati può avere sulle performance energetiche.

Machine learning e predittività: anticipare problemi e agire

Bartolini ha poi approfondito il ruolo sempre più centrale dei modelli predittivi. Grazie a tecniche di machine

learning e deep learning, oggi è possibile rilevare anomalie operative e prevedere guasti di nodi di calcolo con ore di anticipo, anticipare problemi nei sistemi di raffreddamento e stimare in modo più accurato il consumo energetico o le caratteristiche dei job. Questi avanzamenti si basano su dataset di telemetria molto ricchi e articolati, come Exadata, 50 TB di dati raccolti in 31 mesi sul sistema Marconi100, o dataset analoghi relativi al supercomputer Fugaku (Riken), ormai utilizzati a livello internazionale per la ricerca.
Tuttavia, l'accesso a questa mole di dati non è semplice: servono competenze tecniche e di dominio per interrogare i dataset e per interpretarli in modo corretto. È proprio questa complessità che spinge la ricerca verso strumenti più accessibili.

L'AI generativa come interfaccia: dalla query al dialogo

La naturale evoluzione, secondo Bartolini, è l'impiego dell'AI generativa come strumento capace di rendere i dati e i modelli accessibili anche a persone prive di competenze specialistiche. Attraverso modelli sviluppati ad hoc, come ExaAgent ed Exasage, o modelli fondazionali pensati per dati di telemetria e ambienti Kubernetes, diventa possibile interrogare sistemi complessi usando semplicemente il linguaggio naturale.
In futuro, un operatore potrà chiedere al sistema: "Quali job hanno causato l'aumento della temperatura su un determinato nodo nelle ultime 24 ore?", ottenendo una risposta precisa e contestualizzata. L'approccio si basa sull'uso di knowledge graph che rappresentano la semantica dei dati, integrati con componenti capaci di combinare la potenza dei modelli generativi con una solida struttura logica.

Una visione energetica integrata: il data centre come ecosistema

Lo sguardo di Alfonso Capozzoli ha ampliato la prospettiva, riportando al centro il ruolo delle infrastrutture energetiche che rendono possibile il funzionamento dei data centre e per le quali una gestione reattiva non è più sufficiente. Occorre una strategia che metta al centro il monitoraggio, l'analisi avanzata e la capacità di operare una gestione predittiva.
Capozzoli ha mostrato come il Politecnico di Torino abbia adottato un approccio guidato dai dati, potenziando l'infrastruttura di monitoraggio, arricchendo la struttura semantica delle informazioni e rendendole disponibili alla comunità dell'Ateneo. L'obiettivo è trasformare i dati in informazione, e l'informazione in ottimizzazione, favorendo una conoscenza che cresce in modo condiviso e interdisciplinare.

Machine learning e controllo: verso un data centre dinamico e intelligente

Capozzoli ha poi descritto un panorama in cui il machine learning diventa uno strumento attraverso il quale supportare le decisioni e rendere i sistemi più flessibili. I modelli predittivi consentono di rilevare efficacemente anomalie e malfunzionamenti, di stimare la domanda energetica e di programmare le attività di manutenzione in modo più efficiente. Parallelamente, tecniche avanzate di controllo, come i sistemi Model Predictive Control (MPC) o approcci di reinforcement learning, permettono di regolare efficacemente gli impianti a servizio di un data centre e di ottimizzare la prestazione energetica, i costi operativi e la gestione dei campi termici.
Una parte cruciale è rappresentata dai sistemi di climatizzazione, che assorbono spesso una quota significativa dei consumi. Grazie all'analisi continua dei dati e alla simulazione tramite digital twin, è possibile testare scenari alternativi, valutare l'impatto di modifiche ai parametri operativi e individuare interventi che riducano costi e consumi

Grazie alla costruzione di digital twin è stato possibile creare dashboard intelligenti che hanno consentito di ottimizzare i sistemi di raffreddamento con una riduzione dell'8% dei consumi

Andrea Bartolini, Alfonso Capozzoli e Daniela Galetti in occasione del Workshop GARR 2025 che si è svolto a Roma a novembre
Rivedi su GARRtv la sessione dedicata alla sostenibilità

Nei data centre una gestione reattiva non è più sufficiente: occorre una strategia che metta al centro il monitoraggio, l'analisi avanzata e la capacità predittiva

senza compromettere sicurezza e prestazioni. Tecnologie più avanzate come il liquid cooling offrono ulteriori margini di miglioramento.

Un campus come laboratorio: tra visualizzazione e simulazione

Un esempio concreto di questa visione integrata è rappresentato dalla piattaforma Campus Energy Dashboard del Politecnico di Torino.

Approcci diversi con lo stesso obiettivo: una possibile convergenza

di Fabio Farina, GARR

L'approccio presentato offre spunti particolarmente interessanti per le attività del gruppo Data Centre Network di GARR, perché mostra un approccio analogo, ma al tempo stesso complementare, a quello su cui si sta già lavorando. La differenza principale riguarda il punto di partenza: mentre Antares, il sistema multi-agente che automatizza analisi e troubleshooting della rete di data centre GARR, ha un approccio che si concentra sull'analisi delle configurazioni dei sistemi, per individuarne eventuali anomalie, ExaAgent basa la propria metodologia sulla telemetria. Due prospettive diverse, dunque, ma accomunate da un obiettivo comune e da un elemento chiave: l'impiego di agenti di intelligenza artificiale a supporto dell'utente.

Questa complementarità apre scenari promettenti. L'idea di fondere le fonti informative – configurazioni e telemetria – potrebbe infatti fornire una lente di indagine ancora più completa e potente sulle reti dei data centre, permettendo analisi più approfondite e un monitoraggio più efficace.

Un altro elemento di interesse riguarda la possibilità di estendere questa metodologia alla dorsale GARR. La rete GARR-T dispone già di una telemetria molto articolata, che raccoglie un grande numero di dati sullo stato dell'infrastruttura. In questo contesto, il grafo della conoscenza proposto dagli autori trova un corrispettivo naturale nell'inventory automatico degli apparati della rete, che rappresenta in modo strutturato informazioni e relazioni tra elementi.

L'idea di applicare ExaAgent ai dati e alla conoscenza già disponibili su GARR-T apre quindi la strada a sperimentazioni congiunte che potrebbero rivelarsi particolarmente promettenti, portando benefici concreti all'intera comunità.

Costruita interamente con strumenti open source; essa consente un monitoraggio dettagliato dei sistemi energetici e IT e mette a disposizione database temporali, modelli semantici e strumenti di visualizzazione personalizzati per diverse categorie di utenti, dai responsabili della gestione dell'energia e della manutenzione, ai ricercatori.
Nel mock-up dedicato al Datacenter 1 del Politecnico di Torino, dotato di un sistema di contenimento dei flussi di aria calda, sistemi economizzatori indiretti e monitoraggio continuo della potenza IT e delle macchine frigorifere, è possibile analizzare i consumi, calcolare nel tempo metriche di efficienza come il PUE, e rilevare automaticamente anomalie grazie anche a modelli di machine learning. La presenza di un digital twin consente inoltre di simulare diverse condizioni operative e di valutare a priori gli effetti di strategie di controllo predittivo o di variazioni nei parametri operativi di impianto.

Sinergie e direzione futura

Nel dibattito conclusivo sono emersi numerosi punti di connessione tra i due interventi. I dati rappresentano il fondamento comune su cui costruire tanto l'ottimizzazione dei sistemi IT quanto l'efficientamento degli impianti energetici. La semantica e la modellazione avanzata rendono i dati realmente interpretabili e utilizzabili, mentre l'intelligenza artificiale permette di trasformarli in strumenti di supporto decisionale e, sempre più spesso, di controllo autonomo.
Entrambi gli esperti hanno sottolineato quanto la collaborazione multidisciplinare sia fondamentale per affrontare la complessità di infrastrutture che uniscono hardware, software, impianti tecnici e sistemi di gestione. Ed entrambe le visioni convergono verso un futuro in cui l'operatore potrà dialogare in linguaggio naturale con sistemi complessi, ottenendo risposte immediate e ricevendo suggerimenti operativi in tempo reale.

Una visione condivisa per infrastrutture più intelligenti e sostenibili

La sessione si è conclusa con un messaggio chiaro: la sostenibilità dei data centre non è solo un obiettivo tecnologico, ma anche un percorso culturale che richiede il coinvolgimento di comunità diverse e l'integrazione di competenze complementari. L'Italia, grazie alla qualità della ricerca e alla capacità delle sue comunità tecniche di collaborare, ha tutte le carte in regola per giocare un ruolo da protagonista.

Il Digital Twin per la sala macchine di Marconi100: un'applicazione costituita principalmente da due componenti: il data lake che è fornito dal framework ExaMon, sviluppato dall'Università di Bologna ed una applicazione web che fornisce una interfaccia, sia 3D che 2D, sviluppata al Cineca Visit Lab

Data centre: la sostenibilità passa dall'acqua

di Marta Mieli

Liquid cooling nei moderni data centre: tecnologie, sfide e l'esperienza dell'Università di Pisa

La crescente diffusione di tecnologie ad alta intensità di calcolo, dall'intelligenza artificiale al supercalcolo scientifico, passando per big data e realtà virtuale, ha fatto aumentare in modo significativo la potenza dei server e, di conseguenza, la quantità di calore da dissipare. I tradizionali sistemi di raffreddamento ad aria stanno raggiungendo i propri limiti tecnici e non riescono più a sostenere le densità richieste dai nodi di nuova generazione.
Per rispondere a questa sfida, i data centre stanno adottando architetture di liquid cooling che permettono di migliorare l'efficienza energetica, aumentare la densità installabile e garantire continuità di servizio. Un esempio emblematico è il Green Data Center (GDC) dell'Università di Pisa, recentemente ampliato e oggi il più grande data centre universitario d'Italia, che si sta affermando come laboratorio avanzato per la sperimentazione e la messa in produzione di soluzioni innovative per il raffreddamento.
Per approfondire questo argomento abbiamo incontrato **Maurizio Davini**, CTO Green Data Center e **Stefano Suin**, dirigente della Direzione Infrastrutture Digitali dell'Università di Pisa. Con loro analizziamo i limiti delle soluzioni tradizionali, i vantaggi del liquid cooling e le lezioni operative apprese in oltre dieci anni di esperienza sul campo.

Il vostro data centre è il più grande a livello universitario oggi in Italia, quali sono le sue caratteristiche principali?
È vero, siamo all'avanguardia in Europa e l'investimento per realizzarlo è stato davvero strategico per l'Ateneo. Lo scorso anno abbiamo raddoppiato la struttura che si trova a San Piero a Grado: oggi possiamo contare su 104 rack e su un incremento notevole della potenza di calcolo a disposizione della ricerca scientifica dell'università con circa 700 nodi per un totale di circa 30.000 core di calcolo e più di 100 GPU di varie generazioni. Siamo anche l'unico data centre universitario ad aver ottenuto la **classificazione "A"** da parte di AgID. L'obiettivo principale è stato quello di integrare nuovi elementi tecnologici senza snaturare il progetto originale, pensato per avere l'impatto ambientale minore possibile. Grazie alle nuove soluzioni adottate il GDC è in grado di supportare infrastrutture di High Performance Computing (HPC) e di intelligenza artificiale per i prossimi anni, limitando i consumi energetici.

Quali sono i settori che avranno maggior beneficio dal data centre?
L'ampliamento ci ha permesso di compiere un salto di qualità in progetti competitivi di elevato livello e in contesti di frontiera, come il 5G, l'intelligenza artificiale, il quantum computing o il tema dell'High Performance Computing nel contesto del Centro Nazionale finanziato nel PNRR.

Sistemi di così elevata potenza non possono prescindere da una connettività adeguata. È così?
Assolutamente. Abbiamo potenziato la connettività interna ed esterna ad alta velocità ed elevata affidabilità della struttura. Grazie all'attivazione di un **secondo nodo di collegamento alla rete GARR** la potenza di calcolo scientifico è aumentata enormemente. Oggi, infatti, questa struttura può contare su una connettività che consente di sfruttare appieno le sue potenzialità in termini di accesso ai sistemi di HPC e AI e di erogabilità in base alle necessità di ogni progetto;

senza dimenticare la doverosa attenzione alla protezione dei dati e dei risultati della ricerca.

Che scelte avete fatto per raggiungere gli obiettivi di sostenibilità?
Abbiamo adottato soluzioni tecnologiche innovative che permettono l'implementazione del liquid cooling anche in data centre come il nostro che erano già esistenti e che utilizzavano il raffreddamento ad aria.
Abbiamo introdotto, inoltre, **sistemi di calcolo di ultima generazione** come il Lenovo Neptune e i Dell XE, che garantiscono un abbattimento fino al 40% dei consumi di energia senza dover sacrificare le prestazioni. L'Università di Pisa, è stata tra le prime in Europa a adottare queste scelte tecnologiche, facendo del suo Green Data Center una struttura all'avanguardia anche dal punto di vista della sostenibilità ambientale.

Perché è così importante, per la sostenibilità, passare ad una architettura liquid cooling?
Il raffreddamento ad aria è limitato dalla bassa capacità termica e dalla modesta conducibilità dell'aria, che rendono difficile smaltire i carichi crescenti di CPU, GPU e acceleratori. Per mantenere le temperature di giunzione entro le specifiche occorrerebbe aumentare in modo eccessivo portata d'aria, dimensioni dei dissipatori e velocità delle ventole, con impatti negativi su rumore, consumi e affidabilità. In pratica, per i singoli chip oltre 250–300 W per CPU e 400–600 W per GPU/acceleratore il raffreddamento ad aria richiede soluzioni sempre più estreme e poco scalabili. A livello di rack, gli impianti solo ad aria arrivano fino a 30–40 kW/rack con contenimento dei corridoi o rear-door ad aria.
L'evoluzione verso nodi HPC e AI che superano 100–300 kW/rack rende quindi inevitabile l'adozione di sistemi a liquido, in grado di aumentare la densità computazionale mantenendo sotto controllo l'efficienza energetica (PUE, Power Usage Effectiveness) e i costi operativi.
L'esperienza del Green Data Center dell'Università di Pisa conferma che, superata una certa densità, il liquid cooling diventa **una scelta non solo tecnica ma anche strategica**.

L'evoluzione verso nodi HPC e AI rende inevitabile l'adozione di sistemi a liquido, in grado di aumentare la densità computazionale mantenendo sotto controllo l'efficenza energetica e i costi operativi

Noi abbiamo sperimentato un ampio spettro di tecnologie: sistemi bifase dielettrici come ZutaCore HyperCool per nodi ad altissima potenza, soluzioni a micro-getti come JetCool per l'abbattimento degli hotspot e unità di distribuzione del refrigerante (CDU) come Vertiv XDU per la gestione centralizzata dei loop liquidi.

Ci sono diversi tipi di sistemi di raffreddamento?
Esistono due diversi tipi di sistemi: quelli monofase e quelli bifase. Nei **sistemi monofase** il fluido (acqua, acqua-glicole o fluido dielettrico) rimane sempre nello stesso stato; il calore è rimosso tramite convezione forzata in regime turbolento. Sono soluzioni semplici, robuste ed economiche, adatte alla maggior parte dei data centre che operano fino a circa 150 kW/rack con chip nell'intervallo 300–800 W.
I **sistemi bifase**, invece, sfruttano la vaporizzazione locale per assorbire calore tramite calore latente, mantenendo temperature superficiali più stabili e gestendo con maggiore efficacia gli hotspot. Questo approccio risulta particolarmente vantaggioso in presenza di package superiori al kilowatt o in architetture AI ad altissima densità.
Nel nostro data centre, soluzioni bifase dielettriche hanno permesso di semplificare l'infrastruttura facility garantendo prestazioni elevate e isolamento elettrico.

Come funzionano le tecnologie a micro-getti?
Le tecnologie a micro-getti (micro-jet impingement) usano ugelli micrometrici per generare flussi ad alta velocità diretti verso la superficie da raffreddare. L'impatto del getto rompe lo strato limite termico e incrementa sensibilmente

Il raffreddamento direct-to-chip (DTC)

Un sistema DTC trasferisce il calore direttamente dal package al circuito idraulico tramite cold plate dedicati, spesso basati su microcanali. Ogni server integra un loop locale con tubazioni flessibili e raccordi quick-disconnect dripless, collegato a una Cooling Distribution Unit (CDU) che gestisce pompaggio, filtrazione, sensoristica e scambio termico verso il circuito facility. Il Facility Water Loop alimenta le CDU ed è connesso a chiller, dry-cooler e sistemi di free cooling.
Tra i parametri operativi più critici figurano: temperatura del fluido in ingresso (da mantenere sopra il punto di rugiada), portata e ΔT tipici di 5–10 °C per nodo, resistenza termica die–TIM–cold plate, pressione differenziale disponibile e qualità chimico-fisica del fluido.
Al GDC di Pisa, CDU industriali come Vertiv XDU centralizzano controllo, ridondanza e integrazione con il sistema di supervisione dell'impianto.

il coefficiente di scambio, permettendo un raffreddamento estremamente localizzato. I **principali benefici** includono coefficienti di convezione molto elevati, drastica riduzione della resistenza termica locale, gestione efficace degli hot-spot e capacità di dissipare densità di flusso non affrontabili con canali tradizionali.
La **tecnologia JetCool**, basata su micro-convezione, che abbiamo adottato è un esempio concreto applicato a nodi HPC e AI ad altissima densità. L'abbiamo utilizzata per ottimizzare lo scambio termico sui package più critici. Di contro, i micro-getti introducono perdite di carico più elevate e richiedono pompe adeguate, filtrazione fine e un design accurato dell'idraulica interna.

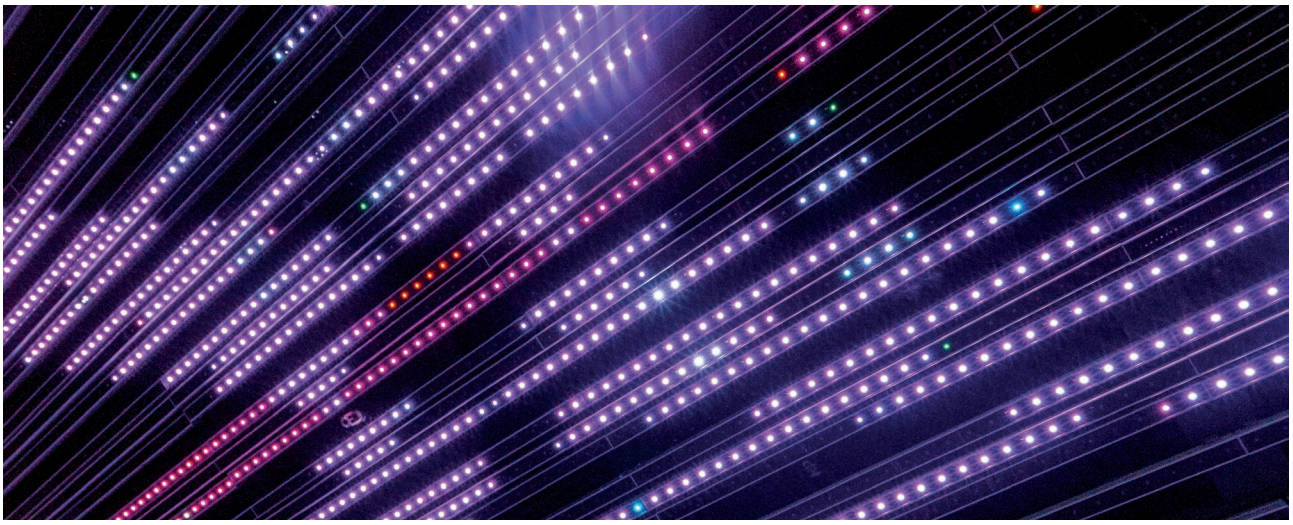
Ci possono essere dei rischi nell'utilizzo dei sistemi a liquido? Cosa occorre fare per prevenirli?
I rischi includono perdite di fluido, corrosione, incrostazioni, biofouling, cavitazione, presenza di aria nel circuito, condensa e, nei sistemi bifase, fenomeni di dry-out o sovrapressioni locali. Le contromisure essenziali comprendono raccordi dripless, leak detection, CDU ridondate N+1, monitoraggio continuo di portata, pressione e temperatura, filtrazione multistadio e procedure di commissioning accurate.
La nostra esperienza sottolinea l'importanza dei test di tenuta iniziali, monitoraggio costante, manutenzione programmata e rigide procedure di emergenza.

Quali sviluppi futuri del liquid cooling appaiono più promettenti?
Tra le principali direttrici evolutive emergono: warm/hot-water cooling a 40–60 °C, soluzioni bifase on-package, microfluidica integrata nel silicio, immersion cooling oltre i 200–300 kW per rack, algoritmi di controllo basati su AI/ML, nuovi fluidi a basso GWP e la progressiva standardizzazione di interfacce e componenti secondo le linee guida OCP (Open Compute Project).
In questa visione, il liquid cooling diventa parte integrante di strategie energetiche più ampie, con benefici in termini di sostenibilità e recupero termico.

Dalla nostra esperienza un elemento chiave è l'integrazione operativa tra team IT e facility. È una condizione indispensabile per gestire in modo affidabile il liquid cooling su larga scala

Quali insegnamenti avete ricavato dalla vostra esperienza?
Sul piano operativo, le lezioni principali riguardano la necessità di un commissioning accurato, il monitoraggio costante tramite BMS/DCIM, la gestione strutturata dei fluidi, piani di manutenzione preventiva e la disponibilità di parti di ricambio. Un elemento chiave emerso dall'esperienza è **l'integrazione operativa tra team IT e facility**, considerata una condizione indispensabile per gestire in modo affidabile il liquid cooling su larga scala.
Queste lezioni costituiscono una base concreta per progettare e gestire data centre di nuova generazione orientati a elevata densità, efficienza energetica e sostenibilità.

• **it.unipi.it**



Innovare nell'età del cambiamento

Dal nuovo piano triennale GARR, una nuova ricetta per guidare l'evoluzione della rete in un contesto in continuo mutamento

di Elis Bertazzon

Da oltre trent'anni, la rete GARR è una delle infrastrutture tecnologiche più solide e innovative del Paese. Ha accompagnato la crescita della ricerca italiana garantendo connettività avanzata, servizi digitali affidabili e una collaborazione continua con le istituzioni scientifiche, accademiche e culturali. Questo rapporto sinergico con la comunità degli utenti è uno dei fattori che ne hanno reso possibile il successo. Oltre ad esso va però ricordato anche un contesto di mercato nel quale operatori economici con spiccate capacità di innovazione e un solido modello finanziario ne hanno supportato l'espansione.

Oggi le condizioni stanno rapidamente cambiando e **un nuovo equilibrio deve ancora delinearsi**: tra un mercato delle telecomunicazioni scarsamente competitivo e innovativo, tecnologie emergenti e dirompenti che richiedono sempre più dati e di conseguenza investimenti costanti, minacce della cybersecurity e un contesto geopolitico internazionale instabile la domanda diventa naturale: come può GARR mantenere il proprio standard tecnologico e garantire al contempo l'indipendenza strategica della comunità della ricerca del Paese?

Il **Piano triennale GARR 2026–2028** risponde con una strategia chiara: investire su infrastrutture più autonome, diversificate e resilienti, su competenze più forti e su un modello collaborativo che metta al centro la comunità degli utenti.

Un mercato diverso: meno concorrenza, più incertezza

Il primo fattore di cambiamento riguarda il mercato delle telecomunicazioni. Stiamo assistendo a una graduale, ma costante, **riduzione della concorrenza** tra i soggetti produttori di mercato. Meno competizione significa meno innovazione, costi crescenti e un rischio maggiore di dipendenza da pochi fornitori.

Un altro cambiamento rilevante è il **progressivo abbandono dei contratti a lungo termine** (a valore predefinito) a favore di modelli basati sul consumo (pay-per-use). Questo approccio, pur introducendo maggiore flessibilità, rende più complessa la pianificazione economica e riduce la prevedibilità dei costi e per un'infrastruttura vasta come GARR, che gestisce oltre 24.000 km di fibra ottica, ciò significa dover ripensare il suo modello tecnologico e economico.

Una duplice sfida

GARR mira a mantenere lo stato dell'arte della tecnologia applicata alla rete e al suo ecosistema e, al contempo, contribuire all'autonomia digitale della ricerca nel Paese.

La sua **strategia si basa su alcuni pilastri**: anticipare i bisogni della comunità scientifica, adottare soluzioni aperte e terabit-ready, ridurre la dipendenza da singoli fornitori con un approccio multi-vendor e valorizzare la comunità degli utenti come parte attiva dell'evoluzione della rete. Ma vediamo cosa prevede il piano.

Il Piano triennale GARR 2026–2028 prevede una strategia chiara: investire su infrastrutture più autonome, diversificate e resilienti, su competenze più forti e su un modello collaborativo che metta al centro la comunità degli utenti

GARR-T come punto di partenza

La rete GARR-T(erabit) rappresenta lo stato dell'arte infrastrutturale. La sua notevole capacità di banda è fondamentale per supportare la scienza dei dati e il calcolo ad alte prestazioni, ed è stata **potenziata con il PNRR** da due interventi strategici nazionali: **ICSC** e **TeRABIT**.

In maniera complementare i due progetti hanno rafforzato il ruolo di GARR come colonna portante della mobilità del dato scientifico, soddisfacendo le esigenze di hyperconnectivity e connettendo risorse di calcolo distribuite su tutto il territorio.

Inoltre, la rete GARR è stata potenziata anche in termini di **resilienza** e **capillarità**. Non è stata solo aumentata la velocità, ma è stata modernizzata l'intera architettura di rete in modo da poter sostenere carichi di lavoro sempre più complessi e distribuiti, assicurando l'accesso universale alle risorse di frontiera per tutta la comunità degli utenti.

Insieme, queste due iniziative hanno costruito una rete pronta a sostenere la scienza dei prossimi anni e già orientata a diventare "a prova di quantum", capace cioè di sperimentare e integrare le tecnologie quantistiche emergenti.

Rafforzamento dell'infrastruttura: multi-vendor e terabit-ready

GARR affronta la sfida del rinnovo di circa 14.000 km di fibra ottica, i cui contratti di concessione d'uso sono in scadenza tra il 2028 e il 2032, con l'obiettivo di garantire continuità di servizio, sostenibilità economica e aggiornamento tecnologico. Il modello monofornitore sarà progressivamente superato in favore di un'architettura multi-vendor più flessibile e scalabile, capace di supportare accessi al terabit grazie alla tecnologia Open Line System di GARR-T.

Parallelamente, GARR intende sviluppare **infrastrutture in fibra transfrontaliera (CBF)** per aumentare la capacità di trasmissione e migliorare la resilienza della rete oltre che ad abilitare a livello internazionale servizi "non data", come il **trasporto di tempo/frequenza**, la **distribuzione di chiavi quantistiche (QKD)**, il supporto al **sensing** distribuito su fibra e al **quantum computing**.

Inoltre, al fine di diversificare ulteriormente l'infrastruttura rispetto alla fibra terrestre, GARR intende estendere la sua **infrastruttura sottomarina**, anche attraverso la collaborazione con altre reti della ricerca, oltre ovviamente a GÉANT e partner industriali per sfruttare la presenza di cavi sottomarini già equipaggiati con tecnologie di nuova generazione (ad esempio, Sparkle o progetto Medusa).

Un elemento centrale nella strategia dei prossimi anni è il supporto al progetto **EuroHPC**, con connettività ad altissima capacità a supercomputer come LEONARDO e i data centre di ECMWF, CINECA e INFN. Per garantire l'accesso ai supercomputer da ricercatori e ricercatrici in tutta Europa e a livello internazionale, GARR avrà un'interconnessione ad altissima capacità e bassa latenza verso la rete GÉANT, inizialmente con un doppio link a 1.2 Tbps ciascuno.

Dal punto di vista tecnologico, **l'attività di sperimentazione** è orientata verso tecnologie avanzate come la distribuzione di chiavi quantistiche (QKD), di tempo e frequenza, il fibre sensing e lo sviluppo di un digital twin della rete stessa.

Oltre alla rete, GARR intende sviluppare un **sistema di object storage** basato sullo standard S3 con un approccio federato, che vede il coinvolgimento diretto delle istituzioni della comunità sia in termini di risorse hardware che umane per la loro gestione e utilizzo..

GARR partecipa attivamente a progetti internazionali e sviluppa **laboratori collaborativi** come il Network OpenLAB insieme a NAMEX, favorendo l'innovazione e la sperimentazione di tecnologie di rete in un ambiente multi-vendor, favorendo l'interoperabilità.

Questo approccio di innovazione aperta è anche uno strumento fondamentale per rendere sostenibili nel futuro gli investimenti: attraverso la ricerca tecnologica e la collaborazione (intesa anche come federazione di risorse), infatti, è possibile mantenere la direzione nello sviluppo della tecnologia senza perderne il controllo strategico.

Leggi il documento completo del Piano di attività triennale 2026-2028

Sicurezza: tra normativa e comunità

Inevitabilmente, in un contesto caratterizzato da minacce cibernetiche crescenti e da obblighi regolatori sempre più stringenti, il piano pone anche un forte accento sull'adeguamento alla **direttiva NIS2** e al **Perimetro di Sicurezza Nazionale Cibernetica (PSNC)**.

Questo impegno non nasce soltanto dall'esigenza di conformità normativa, ma anche dalla trasformazione del mercato della sicurezza, sempre più concentrato e dominato da pochi fornitori. Tale dinamica rischia di generare soluzioni costose, poco interoperabili e orientate più alla certificazione che all'efficacia reale, con un impatto diretto sulla sostenibilità economica dell'infrastruttura.

Per rispondere a questa sfida, GARR intende adottare un **approccio olistico alla sicurezza**, che comprende prevenzione, protezione, rilevamento, risposta e ripristino, e che oltre a soddisfare gli obblighi regolatori, consenta di mantenere un controllo strategico sui costi e sulle tecnologie impiegate. Il PSNC richiede un innalzamento dei livelli di sicurezza e una stretta collaborazione con le autorità nazionali per proteggere le infrastrutture digitali strategiche, ma anche la capacità di selezionare soluzioni aperte, scalabili e realmente efficaci.

La strategia si articola quindi tra miglioramento interno dei processi, standardizzazione e sviluppo di strumenti di cyber hunting, insieme a percorsi di sensibilizzazione e formazione del personale. GARR promuove un modello di sicurezza fondato sulla responsabilità condivisa tra la rete e la sua comunità di utenti, un modello collaborativo che coinvolge attivamente la comunità GARR nella sicurezza, rafforzando resilienza e consapevolezza collettiva e migliorando la capacità di risposta dell'intero ecosistema GARR.

GARR partecipa attivamente a progetti internazionali e sviluppa laboratori collaborativi. Questo approccio di innovazione aperta è fondamentale per rendere sostenibili nel futuro gli investimenti

Il capitale umano e il ruolo chiave della formazione

In un visione di lungo periodo, la formazione è considerata un elemento chiave per l'innovazione e per l'uso efficace delle infrastrutture GARR. L'obiettivo è far crescere le competenze tecniche, sostenere la cultura della sicurezza, valorizzare gli esperti della comunità e introdurre modelli formativi aperti e riconoscibili tramite micro-credenziali. La strategia include **formazione continua** online e in presenza, percorsi strutturati di cybersecurity e collaborazione internazionale.

Una novità in questo senso è l'istituzione di un nuovo tipo di borse di studio per promuovere nuove competenze in settori strategici e rafforzare il legame con gli enti soci. Lo scopo è quello di sviluppare talenti su temi come reti, cybersecurity e AI, inserendoli nell'operatività GARR.

Attraverso la ricerca tecnologica e la federazione di risorse, è possibile mantenere la direzione nello sviluppo della tecnologia senza perderne il controllo strategico

Il Workshop GARR, così come gli altri eventi dedicati agli utenti della rete, rappresenta un momento privilegiato per l'ascolto e la condivisione. La crescita della consapevolezza collettiva è un fattore strategico perché la comunità dell'università e della ricerca continui ad essere parte attiva dell'evoluzione dell'infrastruttura.

Modernizzare l'accesso remoto in ambito accademico: la migrazione di Ca' Foscari a eduVPN

di Stefano Claut

L'Università Ca' Foscari di Venezia ha adottato eduVPN, il servizio internazionale della comunità delle reti della ricerca, migliorando in modo significativo l'esperienza degli utenti: l'accesso remoto è ora più sicuro, immediato e semplice da utilizzare

Negli ultimi anni, all'Università Ca' Foscari ci siamo trovati di fronte alla necessità di ripensare il nostro servizio VPN (Virtual Private Network). La soluzione esistente, nata molti anni fa principalmente per consentire l'accesso alle risorse bibliografiche, nel tempo era diventata difficile da gestire. I profili utente si erano moltiplicati senza un controllo centralizzato, le configurazioni erano complesse e frammentate, e mancava un'integrazione efficace con l'autenticazione a più fattori.
Inoltre, la VPN si basava su dispositivi hardware dedicati, distribuiti su due data centre, una soluzione che risultava poco flessibile e onerosa in termini di gestione e manutenzione. Questa situazione rendeva l'infrastruttura poco adatta alle esigenze moderne di sicurezza, scalabilità e continuità dei servizi, generando difficoltà sia per gli utenti sia per il team tecnico. Il servizio doveva inoltre essere in grado di sostenere un'ampia platea di utenti: l'Ateneo conta circa 30.000 account attivi, tutti abilitati all'uso della VPN, con profili ed esigenze eterogenee.
A fine 2023 abbiamo intrapreso un'analisi approfondita dei profili di utilizzo realmente necessari, con l'obiettivo di individuare una soluzione completamente integrata con il nostro ecosistema digitale. La scelta è ricaduta su **eduVPN Institute Access**, un servizio sviluppato da SURF, la rete olandese dell'istruzione e della ricerca, coordinato a livello europeo da GÉANT e gestito in Italia da GARR.
Per noi è stato un elemento determinante: poter contare su un servizio pensato per la comunità globale della ricerca e supportato a livello nazionale all'interno della rete GARR ha rappresentato un valore aggiunto importante.
L'**integrazione nativa con il Single Sign-On** (nel nostro caso Shibboleth) ha permesso di ereditare automaticamente l'autenticazione a più fattori, l'accesso tramite SPID e CIE e la gestione dei profili basata sugli attributi degli utenti. Tutto questo avviene in maniera trasparente, senza richiedere agli utenti configurazioni complesse o interventi manuali. L'adozione di eduVPN ha quindi semplificato notevolmente la gestione interna, riducendo tempi e costi operativi e migliorando l'esperienza d'uso complessiva.

Un'esperienza semplice e immediata
Uno dei principali punti di forza di eduVPN è la facilità di utilizzo. I client sono disponibili sugli store ufficiali per tutte le piattaforme e non richiedono configurazioni manuali: basta selezionare il proprio istituto

e il resto avviene automaticamente. Questa semplicità ha praticamente azzerato le richieste di assistenza per configurazioni errate, portando benefici immediati sia agli utenti sia al team di supporto IT.
Dal punto di vista tecnico, abbiamo adottato **WireGuard**, che garantisce alte performance e affidabilità anche in condizioni di rete non ottimali o soggette a restrizioni geografiche. In presenza di provider che limitano il traffico UDP, è possibile passare al protocollo TCP direttamente dal client, assicurando così continuità di servizio in qualsiasi situazione.

Un percorso di migrazione graduale
Il processo di adozione è stato pianificato e graduale. Per circa sei mesi abbiamo mantenuto attive sia la vecchia VPN sia eduVPN. Tutte le istruzioni che abbiamo pubblicato sul sito erano relative solamente alla nuova installazione e tutti i nuovi utenti si sono trovati direttamente a utilizzare eduVPN, facilitando così la migrazione. Questo approccio ha permesso una migrazione fluida e senza interruzioni, riducendo al minimo gli interventi manuali.
Abbiamo **installato eduVPN su una singola macchina virtuale**, integrandola nei normali processi di gestione delle VM dell'ateneo, inclusi aggiornamenti, backup, disaster recovery e logging. Questo ha eliminato la complessità dei vecchi apparati fisici e semplificato notevolmente la gestione del servizio, rendendolo più scalabile e facilmente estendibile a nuove esigenze future.
Il servizio è attualmente erogato da una macchina virtuale Ubuntu 24.04 LTS con 4 vCPU e 4 GB di RAM, una configurazione che si è dimostrata più che adeguata per sostenere il carico medio di **circa 250 utenti simultanei giornalieri** e garantire ampi margini di crescita. La soluzione è pensata per essere facilmente scalabile su più VM così da garantire alta affidabilità e migliori performance del servizio. L'efficienza della soluzione ha reso possibile una significativa riduzione delle risorse necessarie rispetto alla precedente soluzione basata su apparati dedicati.

Vantaggi concreti per l'utenza
Oggi eduVPN è l'unico sistema di accesso remoto alle risorse dell'ateneo e viene utilizzato da tutta la comunità istituzionale. Gli **studenti** lo utilizzano per accedere alle risorse bibliografiche, i **docenti** e i **ricercatori** per collegarsi a workstation, cluster e strumenti scientifici, mentre l'accesso di tecnici esterni o ai dispositivi IoT viene autorizzato tramite profili specifici attivati su richiesta. Il servizio ha portato numerosi vantaggi, tra cui una **maggiore sicurezza e privacy**, grazie all'accesso protetto e alla gestione centralizzata degli utenti con autenticazione a più fattori. Garantisce inoltre continuità dei servizi, permettendo di **lavorare anche fuori dal campus**, durante trasferte o esperienze internazionali come l'Erasmus. La gestione è diventata più semplice, riducendo la complessità grazie all'integrazione con l'infrastruttura digitale dell'ateneo.
L'adozione di eduVPN per Ca' Foscari non è stata solo un aggiornamento tecnico, ma anche un cambiamento importante che ha reso l'accesso remoto più sicuro per tutta la comunità accademica. Grazie all'integrazione con i sistemi digitali dell'ateneo e al supporto della rete GARR, il servizio è oggi un elemento fondamentale per l'ammodernamento dell'infrastruttura IT.
Il risultato è un ambiente facile da gestire e pronto a evolversi, in cui studenti, ricercatori e personale interno possono contare su un'esperienza d'uso semplice e senza interruzioni.

• **eduvpn.it**

È stato determinante poter contare su un servizio pensato per la comunità globale della ricerca e supportato a livello nazionale da GARR

Stefano Claut, System Administrator all'Università Ca' Foscari Venezia, è stato tra i protagonisti di Net Makers, l'edizione 2025 del Workshop GARR.
Rivedi su GARRtv il suo intervento nella sessione dedicata ai servizi e applicazioni

Collaborare per la sicurezza: l'esperienza condivisa tra atenei

Un progetto nato dal dialogo tra università per sviluppare strumenti aperti e sostenibili nel monitoraggio degli incidenti informatici

di Erika Trotto

Nel mondo della sicurezza informatica, le sfide si fanno ogni giorno più complesse. Gli attacchi evolvono rapidamente, i servizi digitali si moltiplicano e gli atenei devono riuscire a conciliare apertura e protezione, innovazione e sicurezza. In questo scenario, la collaborazione può fare davvero la differenza: condividere esperienze e competenze permette di affrontare problemi comuni con soluzioni più solide e sostenibili.

Da questa consapevolezza è nata la collaborazione tra il Politecnico di Torino e l'Università "Gabriele D'Annunzio" di Chieti-Pescara, che hanno avviato insieme un progetto dedicato al rilevamento e alla gestione degli incidenti di sicurezza in contesti federati. Un'iniziativa che unisce competenza tecnica e visione strategica, presentata nel corso dell'ultimo Workshop GARR 2025.

Ne abbiamo parlato con **Enrico Venuto**, Coordinatore della Sicurezza Informatica del Politecnico di Torino, e **Damiano Verzulli**, Responsabile della Divisione Informatica dell'Università di Chieti-Pescara.

Un'esigenza concreta e una visione comune

Tutto è partito da un importante cambiamento al Politecnico di Torino. "Abbiamo deciso di spostare l'autenticazione di tutti i nostri servizi, anche quelli cloud, come Microsoft365, su un Identity Provider (IdP) gestito on-premise" spiega Venuto. "In questo modo abbiamo ottenuto un maggiore controllo sugli accessi e una gestione più sicura degli account. D'altro canto, però, abbiamo perso alcune funzionalità di sicurezza avanzata offerte da Microsoft".

Da qui è nata l'idea di sviluppare uno strumento in grado di raccogliere e analizzare gli eventi di autenticazione a tutti i servizi erogati dal Politecnico, inclusi quelli relativi alla piattaforma Microsoft365.

Il cuore del progetto è un sistema distribuito che raccoglie e analizza in tempo reale i log di autenticazione ai servizi d'ateneo. Realizzato interamente con tecnologie open source, permette di individuare anomalie negli accessi e di produrre dati per alimentare un SIEM/SOAR

Abbiamo deciso di lavorare insieme perché volevamo costruire qualcosa che fosse utile non solo ai nostri atenei, ma a tutta la comunità universitaria

Nella situazione di partenza, i log di autenticazione confluivano già su un syslog server centralizzato, gestito secondo il principio della segregation of duties, ovvero, chi lo amministrava non aveva accesso ai sistemi di autenticazione e viceversa, ma le analisi si basavano ancora su strumenti come script in AWK, bash o Python.
L'opportunità di collaborazione tra gli atenei è nata da un incontro con l'Università di Chieti-Pescara in modo naturale, durante un evento tecnico. "È bastata una conversazione per capire che avevamo la stessa visione" racconta Verzulli. "Volevamo costruire qualcosa che fosse utile non solo ai nostri atenei, ma a tutta la comunità universitaria. Così abbiamo deciso di lavorare insieme".

Un modello di lavoro collaborativo

Il cuore del progetto è un **sistema distribuito e basato su microservizi**, che raccoglie e analizza in tempo reale i log di autenticazione ai servizi d'ateneo. Realizzato interamente con tecnologie open source, permette di individuare anomalie negli accessi federati, multifactor e single sign-on, e di produrre dati di qualità per alimentare un SIEM/SOAR dedicato all'Identity Management.
Questo tipo di approccio risponde anche ai requisiti introdotti dalla direttiva NIS2, che richiede agli enti come università e istituti di ricerca di garantire un **monitoraggio continuo degli accessi** e una **gestione strutturata dei log**. La capacità di raccogliere, correlare e analizzare i dati di autenticazione in tempo reale diventa quindi non solo una necessità tecnica, ma anche un elemento fondamentale di conformità normativa.
I log, provenienti dagli IdP, vengono automaticamente filtrati e arricchiti con informazioni aggiuntive — come la geolocalizzazione degli accessi esterni, la classificazione degli accessi interni, la reputazione IP, alcuni indicatori di rischio e diversi altri dati recuperati attraverso API esposte dal sistema informativo interno — per poi essere archiviati su OpenSearch, la piattaforma utilizzata per le successive fasi di analisi e visualizzazione dei dati. Le dashboard interattive consentono di monitorare in tempo reale ciò che accade e di individuare tempestivamente eventuali attività sospette.
La collaborazione si è sviluppata in modo completamente aperto e trasparente: il setup di un'istanza dedicata di Mattermost ha consentito al team di mantenere un flusso di comunicazioni efficiente e ordinato. Parallelamente, un'istanza dedicata di GitLab ha supportato tutta l'attività di sviluppo software. L'infrastruttura è stata interamente gestita con Ansible. Tale approccio ha reso il progetto facilmente replicabile.
Nel giro di pochi giorni sono arrivati i primi risultati concreti, frutto di un'infrastruttura leggera ma molto efficiente.
In tutto questo, la rete GARR ha giocato un ruolo importante: non solo come infrastruttura tecnica, ma come vero e proprio ambiente di collaborazione tra università, enti di ricerca e comunità digitali.
"Sapere di poter contare su una **rete affidabile** e su **servizi condivisi** – sottolineano Venuto e Verzulli – ci ha permesso di concentrarci sull'innovazione, senza reinventare ciò che già funziona".
Il progetto ha portato a un cambiamento significativo nel modo di gestire l'autenticazione e la sicurezza. Da un lato, gli atenei hanno rinunciato a un sistema proprietario potente ma poco flessibile, con funzionalità difficili da personalizzare e limiti nelle ricerche e nei tempi di conservazione dei log. Dall'altro, hanno guadagnato un **punto unico di autenticazione** – multifactor, federato e basato su tecnologie aperte – completamente adattabile alle esigenze dell'ateneo. Un sistema sostenibile, modulare e configurabile, capace di crescere nel tempo insieme ai servizi e alle necessità delle università.

GARR ha giocato un ruolo importante: non solo come infrastruttura tecnica, ma come vero e proprio ambiente di collaborazione tra università, enti di ricerca e comunità digitali

Prospettive future

Il progetto è in costante evoluzione. I due gruppi stanno lavorando per integrare nuove fonti di log – come quelli provenienti da reti Wi-Fi, Active Directory e servizi cloud – e per agevolare l'introduzione di SIEM/SOAR in grado di interfacciarsi ad OpenSearch. Tra le prossime tappe, anche la **sperimentazione di strumenti di intelligenza artificiale** per migliorare l'interrogazione dei dati e il rilevamento automatico delle anomalie.
Alla base di questa esperienza c'è un elemento semplice ma fondamentale: la **fiducia**. "Quando due università decidono di collaborare – sottolinea Verzulli – non condividono solo il codice, ma anche un modo di lavorare, una cultura fatta di apertura e curiosità reciproca". Venuto aggiunge: "Il valore più grande è costruire insieme una cultura della sicurezza, sostenibile e condivisa, che parta dalle persone e cresca grazie alla rete".
In sintesi, l'esperienza del Politecnico di Torino e dell'Università di Chieti-Pescara dimostra che la collaborazione tra atenei può portare a risultati tangibili e innovativi.

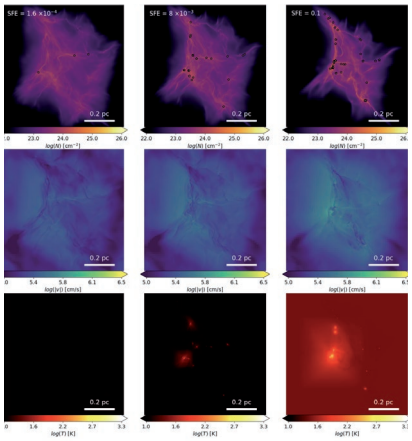
Rivedi su GARRtv la presentazione di Enrico Venuto e Damiano Verzulli in occasione del Workshop GARR 2025

La ricerca comunica

a cura degli uffici stampa degli enti di ricerca

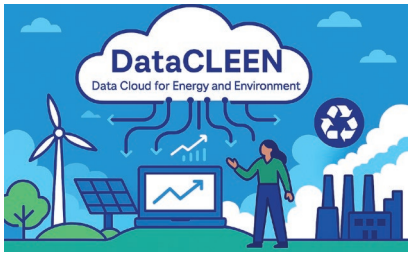
Una “valigia” high-tech per studiare le eruzioni vulcaniche

Durante il convegno mondiale di vulcanologia svoltosi a Ginevra a luglio 2025, l’Istituto Nazionale di Geofisica e Vulcanologia (INGV) ha presentato i risultati di cinque anni di osservazioni ravvicinate delle eruzioni dello Stromboli. Negli ultimi tre anni i ricercatori si sono avvalsi di SKATE (Setup for the Kinematic Acquisition of Explosive Eruptions), un osservatorio portatile delle dimensioni di una valigia, dotato di tecnologie in grado di catturare centinaia di fotogrammi al secondo e di registrare in modo sincrono calore, suono e movimento del fenomeno osservato.
Il sistema, alimentato da batterie sostituibili e pannelli solari, integra un PC impermeabile che coordina una termocamera capace di registrare 32 fotogrammi al secondo e una telecamera ad alta velocità.
SKATE rivoluziona in modo significativo l’osservazione delle eruzioni esplosive, complesse e pericolose, rendendo il processo più efficiente e sicuro.
• ingv.it



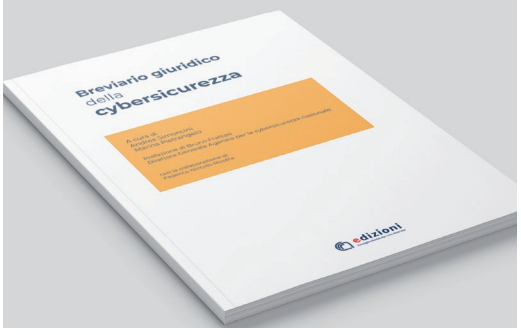
Una “Stele di Rosetta” per la formazione stellare

Coordinato dall’INAF e finanziato dallo European Research Council nell’ambito del Synergy Grant ECOGAL, il progetto Rosetta Stone introduce un approccio innovativo allo studio della formazione stellare: per la prima volta simulazioni numeriche avanzate e osservazioni astronomiche vengono analizzate con gli stessi metodi, creando un linguaggio comune tra teoria e realtà. I primi risultati, pubblicati su Astronomy & Astrophysics, mostrano come le simulazioni possano essere elaborate per riprodurre fedelmente le osservazioni ottenute con strumenti come ALMA e Herschel. Questo permette un confronto diretto e accurato dei parametri chiave che caratterizzano le regioni di formazione stellare, inaugurando una nuova era resa possibile da milioni di ore di calcolo su supercomputer e da una collaborazione stretta tra gruppi teorici e osservativi.
• the-rosetta-stone-project.eu



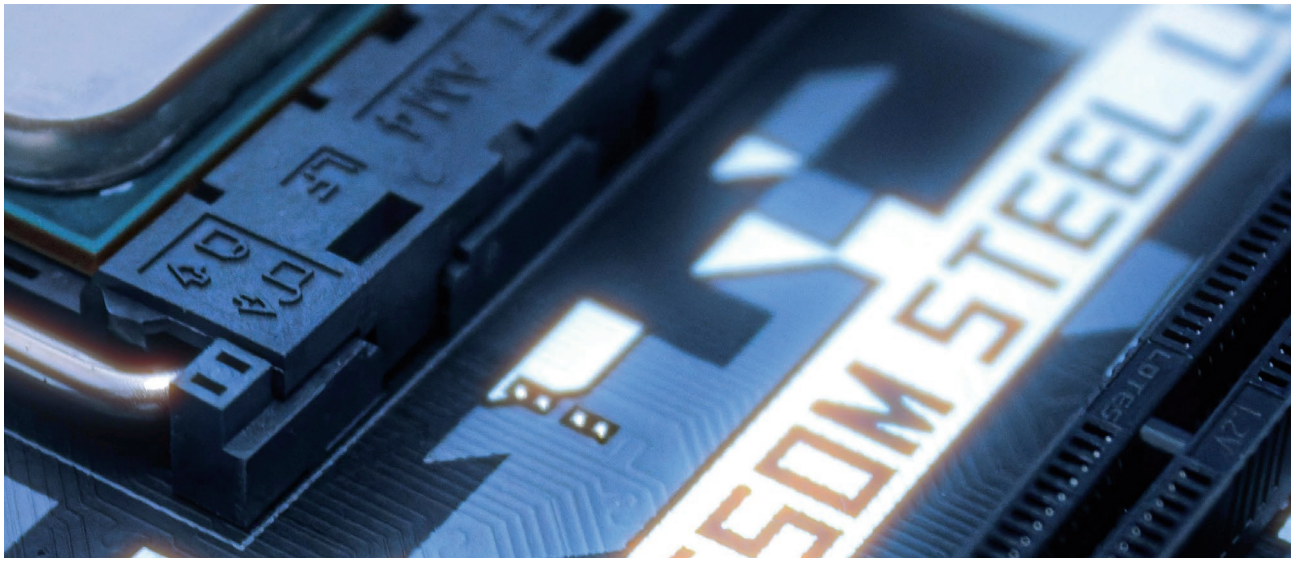
La nuova infrastruttura ENEA per il cloud-edge europeo

Una nuova infrastruttura ad alte prestazioni in grado di integrare tecnologie HPC e servizi cloud di nuova generazione a supporto della ricerca e delle applicazioni industriali più avanzate. È quanto ENEA sta realizzando nell’ambito del progetto DataCLEEN, in linea con l’iniziativa IPCEI-CIS che mira a creare un cloud federato europeo in grado di sviluppare modelli di business basati su intelligenza artificiale (IA) e Internet delle Cose (IoT), promuovendo sostenibilità, competitività, sicurezza e conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR).
Nell’ambito del progetto, ENEA realizzerà quattro nuovi data centre, dotati di elevate capacità di calcolo ed efficienti energeticamente, e potenzierà la connettività tra le sedi con soluzioni di cybersicurezza di ultima generazione.
Questo sistema prevede la creazione e la messa a disposizione di servizi avanzati di intelligenza artificiale, modellistica e gestione dei big data, con l’obiettivo di accelerare la transizione energetica e promuovere lo sviluppo di nuovi prodotti e servizi. Il progetto abiliterà inoltre scenari innovativi in settori ad alto potenziale, tra cui energia, nuovi materiali e smart city.
• 8ra.com/projects/datacleen



Breviario giuridico della cybersicurezza

Pubblicato da Cnr Edizioni Il Breviario giuridico della cybersicurezza, a cura di Andrea Simoncini, professore ordinario di Diritto costituzionale presso l’Università degli studi di Firenze e Marina Pietrangelo, ricercatrice presso l’Istituto di informatica giuridica e sistemi giudiziari del Cnr. Il testo offre una sintesi chiara e rigorosa del quadro normativo europeo e nazionale – dalla NIS alla DORA, dalla CER all’AI Act - e punta alla diffusione della cultura della cybersicurezza come tema non solo tecnico, ma giuridico e istituzionale. Si punta – secondo gli autori - a rendere accessibile una materia complessa senza rinunciare al rigore tecnico-giuridico.
• cnr.it/new_editoriali.it



DNSSEC: un valido aiuto per la sicurezza

di Carlo Volpe

Il Domain Name System (DNS) costituisce un'infrastruttura critica che presenta diverse vulnerabilità che richiedono particolare attenzione, specialmente da parte delle entità classificate come essenziali e importanti nell'ambito della direttiva europea NIS2.
Progettato e messo in esercizio negli anni '80, il DNS originario privilegiava la funzionalità e la velocità a discapito della sicurezza. Data l'enfasi attribuita al servizio DNS dalla normativa europea, GARR ha reso disponibile DNSSEC (Domain Name System Security Extensions) per aumentarne significativamente la sicurezza.
Per capire meglio come funziona DNSSEC, abbiamo intervistato **Marco Gallo**, responsabile dei servizi NIC e LIR di GARR.

Che cos'è esattamente il DNSSEC?
Il DNSSEC è un insieme di estensioni progettate per rendere il protocollo DNS più sicuro. Il DNS tradizionale non verifica l'autenticità delle informazioni né include una prova crittografica che i dati provengano dal nameserver autoritativo legittimo. Se un attaccante riuscisse a modificare i dati scambiati, potrebbe reindirizzare l'utente verso un sito fraudolento. Il DNSSEC risolve questo problema introducendo una catena di fiducia lungo la struttura gerarchica del DNS.

Come funziona questa catena di fiducia?
Ad ogni livello del processo di risoluzione vengono definiti dei passaggi di validazione che consentono di garantire che i dati provengano dal responsabile reale del dominio e che la risposta del DNS non sia stata manomessa.
Per fare questo, il DNSSEC utilizza firme digitali con coppie di chiavi pubbliche e private. La catena di fiducia parte quindi dalla radice del DNS fino ai domini finali: se anche un solo anello della catena non è valido, la risposta viene considerata non affidabile.

Il DNSSEC è un insieme di estensioni progettate per rendere il protocollo DNS più sicuro. Introduce una catena di fiducia lungo la struttura gerarchica del DNS ed è in grado di verificare l'autenticità delle informazioni

Quali tipi di attacchi informatici contrasta?
Il DNSSEC interviene sugli attacchi che prevedono la modifica o la manipolazione dei dati scambiati tra un resolver e un nameserver.
Tra questi abbiamo il cache poisoning, dove l'attaccante inietta record falsi nella cache di un DNS. Il DNSSEC impedisce questo attacco perché il resolver rifiuta qualsiasi record senza firma digitale valida e verificabile.

Un'altra tipologia è il DNS Spoofing: anche se un attaccante intercetta una richiesta e risponde con un IP falso, un resolver con DNSSEC attivo ignora la risposta a meno che essa non includa firme DNSSEC valide.
Poi c'è la Falsificazione di Inesistenza (NXDOMAIN): il DNSSEC estende la protezione alla negazione di esistenza di un dominio (NXDOMAIN). Utilizza i record NSEC/NSEC3 per creare una prova crittografica che un nome non esista all'interno di una zona.

DNSSEC serve anche per proteggere la privacy delle richieste?
No, il DNSSEC **non è un protocollo di cifratura e non protegge la privacy** delle richieste DNS né impedisce l'intercettazione (sniffing) dei pacchetti. Per la riservatezza, è necessario affiancarlo con protocolli di crittografia come il DoH (DNS over HTTPS) o DoT (DNS over TLS).
Inoltre, DNSSEC non protegge dagli attacchi DDoS (Distributed Denial of Service). Non è stato progettato per bloccare o gestire l'enorme volume di traffico generato da un attacco di questo tipo. Al contrario, l'aumento della dimensione dei pacchetti di risposta richiede una configurazione attenta senza la quale i server DNSSEC potrebbero essere sfruttati involontariamente come amplificatori in attacchi di tipo reflection/amplification contro terze parti.

Come si attiva la Chain of Trust?
Per gli enti GARR, l'attivazione inizia con una richiesta via email a nic@garr.it. Il processo richiede che GARR aggiorni la delega del nome a dominio presso il database delle Authority dei TLD.
Il funzionamento è leggermente diverso per i domini .it e .eu. Per i primi chi gestisce il nameserver master della zona deve generare il record DS. GARR lo riceve e lo trasmette al Registro .it, che lo inserisce nella zona .it.
Per i domini .eu, invece, chi gestisce il nameserver master deve trasmettere la chiave pubblica KSK associata alla zona firmata. GARR inoltra la chiave pubblica a EURid che, per evitare errori di generazione dell'hash, genera autonomamente il record DS.

Quali consigli daresti a chi vuole adottare DNSSEC?
Sebbene la complessità di DNSSEC possa preoccupare, i moderni software DNS offrono funzionalità di automazione che ne semplificano la gestione. Dopo l'attivazione, **l'attenzione va concentrata sul monitoraggio** per assicurare stabilità ed efficienza. È fondamentale, infatti, monitorare l'impatto dell'aumento del payload dei pacchetti DNS sui firewall. Risposte troppo grandi possono innescare il fallback da UDP a TCP, introducendo latenza. Inoltre, è opportuno monitorare l'impatto prestazionale sui server autoritativi, verificando l'uso di risorse come RAM e carico della CPU dovuto alla maggiore necessità di potenza di calcolo.
La sicurezza operativa si basa poi sulla **protezione delle chiavi private**, in particolare la KSK. L'ideale è custodire le chiavi private su un dispositivo isolato dalla rete o utilizzare un HSM (Hardware Security Module), che custodisce le chiavi e firma i dati internamente, prevenendo l'esposizione.

Il DNSSEC interviene sugli attacchi che prevedono la modifica o la manipolazione dei dati scambiati tra un resolver e un nameserver

In conclusione, DNSSEC è davvero così importante?
Chi gestisce un dominio e intende offrire un servizio affidabile non può ignorare il DNSSEC. È una componente fondamentale per la resilienza dell'infrastruttura. L'adozione di DNSSEC è cruciale per la **conformità con la direttiva NIS2** poiché contribuisce a garantire la disponibilità e la continuità operativa del servizio, stabilendo un solido standard per la sicurezza delle reti e dei sistemi informativi.

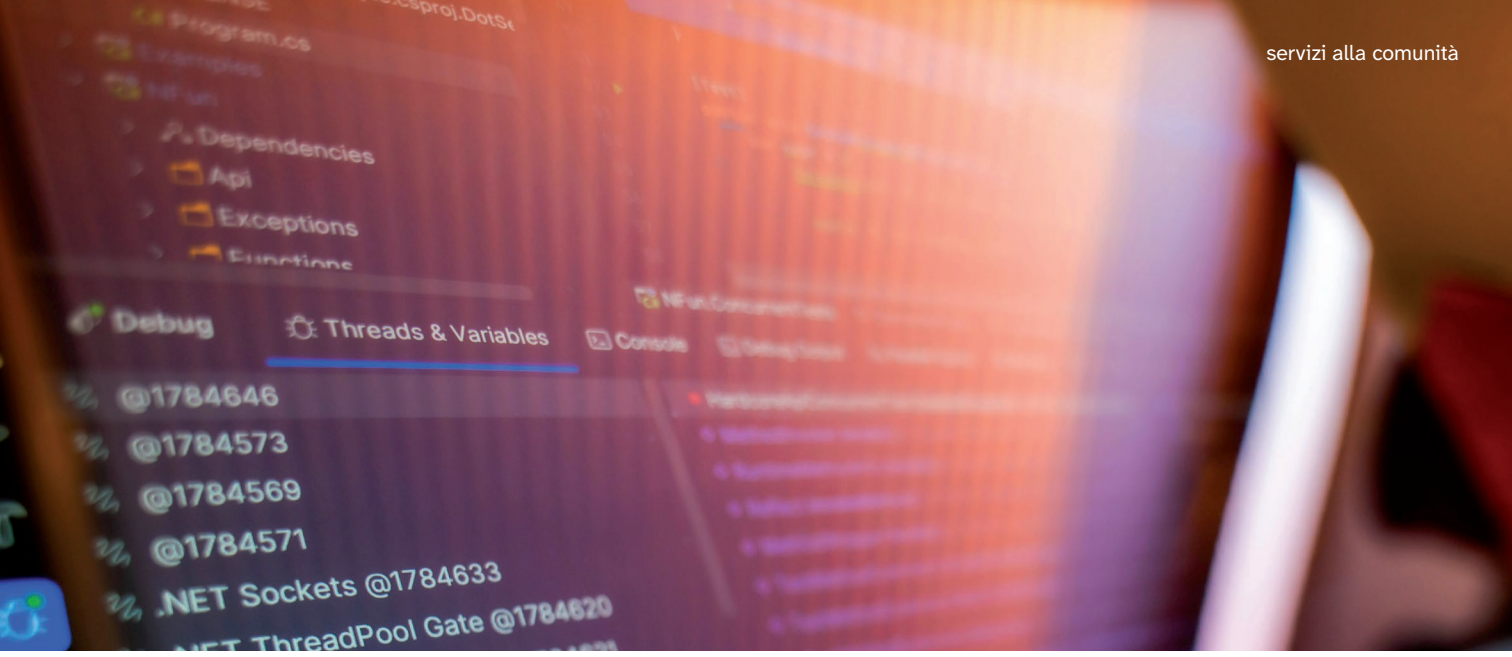
• nic.garr.it

Come avviene il processo di validazione

Il DNSSEC utilizza coppie di chiavi asimmetriche (pubblica e privata) per generare firme digitali che garantiscono l'autenticità dei dati.

- **Zone Signing Key (ZSK) privata:** genera le firme digitali (RRSIG) che coprono i set di record della zona figlio (es. i record A, MX, TXT).
- **ZSK pubblica:** inclusa nel record DNSKEY della zona, è usata dai resolver validanti per verificare l'integrità delle firme RRSIG.
- **Key Signing Key (KSK) privata:** utilizzata per firmare l'insieme delle chiavi pubbliche della zona (il set di record DNSKEY), inclusa la ZSK pubblica.
- **KSK pubblica:** utilizzata dal resolver per verificare la firma della KSK privata sull'insieme delle chiavi (DNSKEY RRSet). Inoltre, il suo hash viene pubblicato come record DS (Delegation Signer) nella zona padre (es. TLD .it).

Quando un resolver (con DNSSEC attivo) riceve una risposta, esegue un processo di validazione gerarchico. Dopo aver collezionato i record, il resolver usa la ZSK pubblica per verificare l'RRSIG associata al record.
Questa verifica non basta, poiché un attaccante potrebbe alterare anche la chiave KSK se questa non è fidata. Per verificare l'autenticità della KSK, il resolver risale alla zona padre dove il register di dominio (es. GARR) ha caricato il record DS.
Il resolver confronta il record DS con l'hash della KSK Pubblica della zona figlio. Se c'è corrispondenza, il primo anello della Catena di Fiducia è stabilito. Questo meccanismo si ripete fino alla Root.
Al livello più alto, poiché non esiste un dominio padre sopra la Root, la catena termina con la Trust Anchor. Questa è la chiave pubblica KSK della Root, che è pre-configurata nel software del resolver.
Con la validazione successiva della KSK della Root tramite la Trust Anchor, il resolver completa il processo. Una volta validato con successo ogni anello, il record è contrassegnato come "secure" e viene restituito al client.



TCS GARR: un tool di automazione per i certificati digitali

di Carlo Volpe

I certificati digitali rappresentano le fondamenta della fiducia su Internet, garantendo autenticazione e protezione delle comunicazioni in rete. Permettono, infatti, di verificare l'identità di un sito o di un'organizzazione e di cifrare il traffico proteggendo dati sensibili come password, dati personali o transazioni economiche.
Dietro questi certificati ci sono le cosiddette Certificate Authority (CA), autorità che verificano l'identità dei richiedenti e rilasciano i certificati.
Negli ultimi anni il mercato globale dei certificati digitali è cresciuto in modo significativo, ma, secondo il report "Market concentration" di Internet Society, è tra i servizi di Internet maggiormente soggetti a dinamiche di forte concentrazione. In questo settore, infatti, la posizione dominante di poche CA è molto evidente e di fatto, tante organizzazioni e siti web dipendono da un numero relativamente ristretto di autorità per ottenere i certificati digitali.
Nel 2025 la comunità della ricerca europea, tramite GÉANT, ha scelto di affidarsi a HARICA (Hellenic Academic and Research Institutions Certification Authority), una CA che nasce in un ambiente universitario ed è finanziata da Greek Universities Network (GUnet), un'organizzazione senza scopo di lucro i cui membri sono le università della Grecia.
Come ogni cambio di gestore, dal punto di vista tecnico, è stato necessario effettuare una serie di adattamenti dovuti alle diverse modalità di fornitura del servizio.
In particolare, all'inizio del contratto, da gennaio a giugno 2025, HARICA non aveva ancora implementato il supporto al protocollo ACME (Automated Certificate Management Environment), ovvero uno standard dell'IETF che consente di automatizzare l'intero ciclo di vita dei certificati digitali SSL/TLS, dalla richiesta al rinnovo.

Nel 2025 la comunità della ricerca europea si è affidata ad HARICA, una Certificate Authority che nasce nell'ambiente universitario in Grecia

Per i SysAdmin, abituati ad automatizzare il processo per evitare rinnovi manuali, questa mancanza rappresentava una criticità operativa notevole.
Per colmare questo vuoto, GARR ha sviluppato la soluzione TCS GARR Client, un tool a riga di comando (CLI) progettato per interagire con le API di HARICA, facilitando le operazioni massive che l'interfaccia web non poteva garantire.
Per saperne di più abbiamo incontrato **Pasquale Mandato**, responsabile del gruppo IT di GARR e **Vincenzo Caracciolo**, DevOps engineer di GARR.

Il report *Market concentration* di Internet Society è disponibile al link: pulse.internetsociety.org/concentration

Il progetto TCS GARR è disponibile su GitHub all'indirizzo: github.com/ConsortiumGARR/tcs-garr

Come avete reagito all'assenza di strumenti di automazione?
Mandato. Sapevamo che non potevamo tornare a gestire i certificati a mano. Abbiamo studiato le API di HARICA e, ben prima dell'avvio ufficiale del contratto, abbiamo iniziato a sviluppare un client che permettesse di fare tutto da riga di comando. L'obiettivo era azzerare il disagio del cambio del fornitore.

Che cos'è, in pratica, il client TCS GARR?
Caracciolo. È uno strumento open source scritto in Python che fa da ponte tra gli utenti e la CA permettendo agli amministratori IT di eseguire operazioni avanzate direttamente da terminale: dalla richiesta e approvazione dei certificati alla gestione delle identità ACME, fino all'esportazione di report dettagliati.

Come si è arrivati allo sviluppo del tool?
Mandato. Siamo partiti analizzando le poche soluzioni sperimentali esistenti in ambito internazionale e abbiamo deciso di sviluppare qualcosa di più maturo.
Abbiamo iniziato a lavorare ben prima dell'inizio operativo del contratto con HARICA per non lasciare gli utenti con un vuoto tra un provider e l'altro. La prima release è stata a gennaio, quindi siamo riusciti ad essere molto tempestivi.
Caracciolo. In una fase successiva abbiamo sviluppato un'immagine Docker di tcs-garr, pensata come base comune per agevolare lo sviluppo di altri strumenti e semplificarne l'utilizzo. Su questa base abbiamo realizzato auto-harica, un tool in grado di simulare il comportamento di un client ACME, sopperendo alla sua assenza fino al rilascio ufficiale avvenuto nel mese di luglio.

Quali sono le principali funzionalità?
Mandato. Il client offre un set completo di comandi per l'amministrazione quotidiana. Permette, infatti, di richiedere certificati tramite richiesta di firma del certificato (CSR) o con generazione automatica, di approvare o cancellare richieste, di elencare certificati con filtri avanzati (stato, scadenza, FQDN, proprietario), di scaricare certificati in formato pemBundle o certificate, di revocare certificati (solo API). Nella gestione del protocollo ACME consente di elencare gli account ACME, creare nuovi account, disabilitarli, ottenere token e regole di validazione dei domini.
Il tool inoltre permette la validazione dei domini generando i token di validazione necessari per completare le verifiche richieste dalla CA.
Caracciolo. Tra le altre caratteristiche, inoltre, è previsto il supporto Kubernetes con la possibilità di generare direttamente file YAML di tipo Secret per importare certificati TLS in cluster Kubernetes e altre funzionalità come la notifica automatica, ad esempio verso Slack, alla richiesta di un nuovo certificato e strumenti diagnostici per interrogare endpoint specifici e verificare la corretta comunicazione con le API di HARICA.

TCS GARR è un tool open source scritto in Python che permette agli amministratori IT di eseguire operazioni dal terminale: dalla richiesta e approvazione dei certificati alla gestione delle identità ACME, fino alla creazione di report dettagliati

Come può essere installato il client?
Caracciolo. Abbiamo progettato il tool per essere agnostico e facile da installare, sia via pip, pipx che tramite Docker sfruttando le immagini pubblicate nel GitHub Container Registry.

Con quale licenza è rilasciato il software?
Caracciolo. Il progetto è rilasciato come software open source (GPLv3) ed è disponibile su PyPI e come immagine Docker. Chiunque può contribuire con nuove funzionalità, segnalazioni o patch. Sono già presenti vari contributori attivi, e il progetto è pensato per crescere grazie alla collaborazione della comunità accademica e della ricerca.
Pur essendo distribuito da GARR, il software non è ufficialmente supportato né approvato da HARICA, e viene offerto alla comunità senza garanzia di manutenzione o supporto.

Come è stato accolto dalla comunità?
Mandato. Il riscontro della comunità è stato molto positivo. Ad oggi contiamo circa 39.000 download del software da GitHub, un dato che testimonia il forte interesse verso il progetto. Abbiamo ricevuto diverse pull request e segnalazioni di bug dagli utenti, confermando che il tool non è solo utilizzato, ma attivamente migliorato dalla comunità accademica.
Caracciolo. In alcuni casi abbiamo dato supporto per l'installazione, e ciò è stato particolarmente utile. All'Università di Trento, ad esempio, anche utenti non esperti di Python in pochi minuti sono riusciti a rendere operativo il tool e ciò ha risolto i problemi di esperienza utente che c'erano con HARICA. Le funzionalità più apprezzate sono state la generazione di nuovi certificati, l'automazione dei rinnovi, le revoche e la possibilità di fare le Domain Validation (DV) tramite script.

• ca.garr.it

Ad oggi contiamo circa 39.000 download del software da GitHub, un dato che testimonia il forte interesse verso il progetto

Leggi la documentazione del servizio su:
tcs-docs.aai.garr.it

PACMAN: l'automazione che sta cambiando la rete GARR

Il configuration manager che ha rivoluzionato il provisioning e la configurazione della rete a pacchetto GARR-T, raccontato attraverso le voci di chi lo ha progettato e lo utilizza ogni giorno

di Erika Trotto

L'automazione nelle reti moderne è diventata un elemento imprescindibile. In contesti in cui l'infrastruttura cresce per dimensioni, servizi, velocità e complessità, affidarsi a operazioni manuali non è più sufficiente. La rete GARR non fa eccezione: negli ultimi anni, grazie al progetto GARR-T, è diventata più potente e articolata, ma anche più difficile da gestire con gli strumenti tradizionali basati su riga di comando (CLI).
Da questa necessità è nato **PACMAN**, il PAcket layer Configuration MANager, un framework sviluppato con l'obiettivo di trasformare il modo in cui vengono generate, validate e applicate le configurazioni dei router del backbone.

Dalle prime sperimentazioni al 100% di automazione
Quando PACMAN è stato presentato per la prima volta al Workshop GARR del novembre 2024 copriva appena il 30% dei router della rete a pacchetto. Nonostante fosse già stato riconosciuto come un passo avanti significativo, nessuno poteva prevedere la rapidità con cui sarebbe diventato lo strumento principale per la gestione dell'intero backbone della rete GARR-T.
Nel corso di dodici mesi il progetto ha visto un'estensione progressiva dei modelli di servizi supportati, la risoluzione sistematica dei bug emersi e, soprattutto, l'integrazione diretta con NetBox, che oggi permette di monitorare lo stato di conformità dei router sia tramite viste di insieme che tramite dettagli puntuali.
Il passaggio più importante è stato tuttavia quello **culturale**. La completa automazione dei router della rete di produzione, traguardo celebrato con un momento dedicato a tutto il team, è stata raggiunta grazie alla collaborazione di gruppi diversi: i team Data Centre Network, IT ed il GARR NOC (Network Operations Centre). Il risultato non è la sola adozione di un nuovo software, ma la **costruzione di un modello operativo condiviso**, basato su strumenti comuni e processi uniformi.
La crescita della rete GARR aveva messo in evidenza i limiti del modello manuale di gestione. La configurazione dei router richiedeva interventi puntuali, spesso ripetuti e soggetti a variabilità. PACMAN introduce un approccio simile

PACMAN permette di definire in modo astratto le configurazioni della rete e trasformarle automaticamente in configurazioni reali pronte per essere distribuite sui router

Prima era necessario intervenire su ogni router, ora l'intera infrastruttura può essere gestita in maniera coerente, con maggiore stabilità operativa e visibilità completa sul backbone.

a quello dello sviluppo software: astrazione del design, controllo di versione, pipeline automatizzate e coerenza tra le configurazioni desiderate e quelle realmente applicate.
Per comprendere la portata del cambiamento, ci siamo confrontati con **Giancarlo Viola**, responsabile del gruppo Data Centre Network, e con **Fabrizio Bataloni**, responsabile del NOC, che ogni giorno vivono sul campo i risultati di questo percorso.

Cos'è PACMAN e come funziona

Giancarlo Viola spiega che PACMAN "permette di definire in modo astratto le configurazioni della rete e trasformarle automaticamente in configurazioni reali, pronte per essere distribuite sui router Juniper".
Le configurazioni vengono descritte in YAML, mentre la generazione dei file finali passa attraverso template Jinja2, che garantiscono uniformità e riducono la possibilità di errori. Questa **separazione tra design e operatività** consente una maggiore uniformità dei servizi di rete offerti agli utenti e una gestione più semplice, e allo stesso tempo efficiente, dell'intera infrastruttura di rete.
Il framework, basato su Ansible, costruisce, valida e applica le configurazioni attraverso workflow completamente automatizzati. Ogni modifica è tracciata, ogni configurazione può essere verificata rispetto ai modelli di riferimento e l'integrazione con NetBox permette di monitorare costantemente la conformità dei dispositivi. **È un approccio DevOps applicato a una rete nazionale complessa**.
Per il NOC, come racconta Fabrizio Bataloni, il cambiamento è stato evidente fin da subito. Prima era necessario intervenire router per router. Ora l'intera infrastruttura può essere gestita in maniera coerente, con maggiore stabilità operativa e visibilità completa sul backbone.
Uno dei momenti più significativi è stato il raggiungimento della **completa automazione del backbone**. All'inizio, PACMAN veniva impiegato solo per una parte limitata della rete, ma nel tempo è diventato lo strumento unico per la gestione di tutti i router. Secondo Viola, questo dimostra come metodologie tipiche dello sviluppo software – pipeline CI/CD, controllo delle versioni e gestione del ciclo di vita – siano applicabili con successo anche a una rete nazionale.
Viola sottolinea che questo risultato non sarebbe stato possibile senza un vero cambio culturale. L'automazione richiede un **linguaggio condiviso e strumenti comuni**. Il traguardo è stato raggiunto grazie a un lavoro multidisciplinare che ha unito competenze diverse in un obiettivo comune.

Vedi la presentazione di Giancarlo Viola al Workshop GARR 2025 dal titolo "Network Automation"

Dalla rete di produzione ai data centre

L'esperienza maturata su GARR-T ha permesso di estendere la stessa filosofia anche ai data centre GARR. Qui esisteva già un modello automatizzato per gli apparati Arista, ma mancava un sistema equivalente per la componente Juniper. È così nato **PACMAN DCN**, che oggi permette di gestire automaticamente gli apparati dei data centre INFRA e dei siti della cloud GARR (Napoli, Catania, Palermo), uniformando tecnologie e modelli operativi. L'automazione nei data centre, avviata già anni fa, è stata così completata. Oggi **tutti i data centre GARR adottano un modello coerente**: AVD (Arista Validated Designs) per gli apparati Arista, che consente di generare e distribuire automaticamente configurazioni uniformi e ripetibili, PACMAN DCN per la componente Juniper. Questo garantisce **omogeneità delle configurazioni di rete e riduzione dei tempi legati all'operatività**. La stessa logica è stata applicata anche alla LAN della Direzione, creando PACMAN Direzione: un progetto che adotta gli stessi workflow usati nel backbone e nei data centre. Ne risulta un ecosistema ribattezzato internamente "galassia PACMAN" che comprende tre progetti principali: la gestione della rete di produzione, la gestione dei data centre e la gestione della LAN della Direzione.

Le sfide future

L'evoluzione non si ferma. Uno dei prossimi obiettivi è l'automazione dei CPE (Customer Premises Equipment), cioè dei dispositivi di rete installati presso gli utenti finali, governati da GARR. È già stato avviato **PACMAN CPE**, dove si sta sperimentando come modellare gli apparati Cisco secondo lo stesso paradigma utilizzato per i router Juniper. Parallelamente, si lavora all'integrazione con il workflow orchestrator. Questo permetterà di descrivere i servizi di rete direttamente all'interno dell'orchestratore e distribuire automaticamente le configurazioni tramite PACMAN, costruendo un processo completamente end-to-end: dalla definizione del servizio alla sua implementazione sui dispositivi.
PACMAN non è solo un software: è l'espressione di un'evoluzione metodologica, organizzativa e culturale. Ha richiesto apertura mentale e collaborazione costante tra team diversi, introducendo nella gestione della rete approcci propri del software engineering. Oggi la rete GARR è più complessa e più potente, ma anche più prevedibile e gestibile, grazie a un framework che ne ha trasformato radicalmente il modo di progettare, distribuire e controllare le configurazioni.

PNRR: il bilancio dei progetti TeRABIT e ICSC e il ruolo strategico di GARR

di Sara Di Giorgio

TeRABIT e ICSC: due progetti per una nuova infrastruttura nazionale

Nell'ambito del Piano Nazionale di Ripresa e Resilienza, i progetti **TeRABIT** e **ICSC** rappresentano due interventi strategici per il rafforzamento dell'infrastruttura digitale nazionale, avviati rispettivamente il 1° gennaio 2023 e il 1° settembre 2022. I due progetti prevedono un investimento complessivo superiore ai 360 milioni di euro (41 milioni per TeRABIT e 320 milioni per il Centro Nazionale ICSC), con una quota GARR pari a circa 17,7 milioni per TeRABIT e 15 milioni per ICSC. Grazie a questi interventi, l'Italia ha potuto rinnovare la propria rete nazionale della ricerca, aumentare la capacità di calcolo e consolidare un ecosistema dedicato a HPC, Big Data e tecnologie quantistiche. GARR ha completato le proprie attività nei tempi progettuali (marzo–giugno 2025), senza essere interessato dalle proroghe dei due interventi. I progetti ICSC e TeRABIT si avviano alla conclusione ad aprile 2026.

Questo risultato pone il Paese in una posizione particolarmente favorevole nel contesto europeo. L'economia globale sta attraversando una trasformazione profonda: dalla produzione di beni materiali si è passati alla produzione di nuova conoscenza, un ambito sempre più dominato dalle grandi aziende specializzate in intelligenza artificiale e attraverso l'uso massivo di tecnologie GPU.

In questo scenario, l'Europa sconta un ritardo competitivo significativo. Il **Rapporto Draghi** (settembre 2024) ha evidenziato la necessità urgente di aumentare la capacità di calcolo, investire in infrastrutture HPC e sostenere lo sviluppo di modelli avanzati di intelligenza artificiale. TeRABIT e ICSC, avviati prima della pubblicazione del rapporto, anticipano molte di queste raccomandazioni e consentono oggi all'Italia di presentarsi con un'infrastruttura digitale moderna, scalabile e pienamente coerente con le priorità europee.

La rete GARR conta oltre 120 punti di presenza e raggiunge oggi una capacità complessiva di circa 36 Terabit al secondo sulla dorsale

In entrambi i progetti, **GARR ha svolto un ruolo determinante**. All'interno di TeRABIT e ICSC ha guidato la realizzazione della nuova dorsale ottica nazionale ad altissima capacità in nuove aree come la Sardegna e l'Abruzzo, completando la transizione delle aree del Sud Italia alla rete GARR-T e garantendo la connettività avanzata necessaria al funzionamento coordinato dei centri di calcolo distribuiti sul territorio. L'impatto combinato dei due progetti ha permesso di aumentare in modo significativo le prestazioni delle infrastrutture nazionali e di creare un ecosistema digitale coerente, interoperabile e competitivo a livello europeo.

TeRABIT: la nuova infrastruttura digitale del Paese

GARR-T ha segnato un passaggio fondamentale nell'evoluzione dell'infrastruttura di rete nazionale. Il progetto TeRABIT, ha consentito di integrare e potenziare **tre asset strategici:** la rete GARR-T, il sistema HPC PRACE-Italy e l'infrastruttura distribuita HPC-BD-AI dell'INFN. GARR ha messo a fattor comune tecnologie ottiche di ultima generazione e un'architettura più flessibile e scalabile per i servizi di rete. La nuova configurazione ha migliorato la resilienza, incrementato la capacità trasmissiva e introdotto strumenti avanzati di automazione e orchestrazione.

La rete GARR raggiunge oggi una capacità complessiva di circa 36 Terabit al secondo sulla dorsale e conta oltre 120 punti di presenza distribuiti su tutto il territorio nazionale, con un'estensione complessiva della fibra pari a oltre 24.000 chilometri, risultando la più estesa infrastruttura di connettività per la ricerca e l'istruzione in Europa secondo i dati del report annuale della rete europea GÉANT.

Particolarmente significativo è l'intervento realizzato in **Sardegna** attraverso il progetto TeRABIT, che ha reso operativo

un **nuovo anello in fibra di circa 1.100 chilometri** e, grazie all'acquisizione di spettro su **due cavi sottomarini**, ha consentito la realizzazione di quattro collegamenti a 400 Gbps verso la dorsale, garantendo l'integrazione dell'isola nella rete nazionale alle stesse condizioni operative del continente, con una capacità aggregata verso la regione di 1,6 Tbps ulteriormente scalabile. Il sito candidato per l'Einstein Telescope è già oggi connesso alla rete GARR-T tramite due collegamenti a 100 Gbps; il potenziamento dell'infrastruttura regionale rappresenta quindi un passo strategico per assicurare, nel medio periodo, la disponibilità di connessioni ad altissima capacità e bassa latenza, prerequisito essenziale per le future esigenze scientifiche del progetto.

TeRABIT ha inoltre consentito il potenziamento di numerosi punti di presenza GARR sul territorio nazionale. La migrazione verso la nuova infrastruttura ha richiesto un intenso coordinamento operativo, garantendo la continuità dei servizi di rete anche nelle fasi più delicate.

Nell'ambito del progetto TeRABIT, nell'infrastruttura distribuita dell'INFN sono state introdotte le cosiddette **bolle HPC**, nodi di calcolo collocati in prossimità dei luoghi di produzione dei dati e collegati alla rete nazionale ad alta capacità. Tale approccio consente di avvicinare le risorse computazionali agli utenti, supportando modelli data-intensive e migliorando l'efficienza dei flussi di elaborazione. La creazione della federazione cloud nazionale garantisce inoltre standard uniformi di accesso, interoperabilità e sicurezza, in linea con le principali iniziative europee come EOSC e EuroHPC.

ICSC: il Centro Nazionale del supercalcolo

Il progetto ICSC si configura come uno dei principali interventi nazionali dedicati a supercalcolo, gestione dei dati e tecnologie quantistiche. Il progetto è organizzato con un hub centrale che gestisce la parte amministrativa e undici spoke che hanno il compito di implementare il programma. La struttura con uno spoke trasversale responsabile del potenziamento e della gestione dell'infrastruttura tecnologica (spoke 0) e dieci spoke tematici ha consentito di mettere a sistema un ampio insieme di competenze scientifiche e infrastrutture di calcolo distribuite tra università, enti pubblici di ricerca e partner industriali.

GARR partecipa allo spoke 0, assicurando la **connettività avanzata** indispensabile per la federazione dei centri di supercalcolo. La rete GARR-T rappresenta infatti l'elemento abilitante per l'accesso omogeneo alle risorse HPC, oggi distribuite in tutto il Paese. Grazie all'infrastruttura rinnovata, è stato possibile consolidare e potenziare sistemi di rilevanza internazionale come il supercomputer Leonardo, incrementato grazie al sistema LISA del 30% in potenza computazionale, e i centri dedicati ai Big Data dell'INFN. Inoltre, sono stati creati due nuovi centri dedicati alla Space Economy ai Laboratori Nazionali di Frascati e alla resilienza ai disastri naturali ed antropici ai Laboratori Nazionali del Gran Sasso. Infine, il Tecnopolo di Bologna ha accolto il **primo sistema quantistico italiano**, integrato nell'ecosistema ICSC per lo sviluppo di applicazioni ibride.

La rete nazionale è stata completamente rinnovata nelle sue componenti ottiche e di trasporto, con particolare attenzione alle regioni del Mezzogiorno

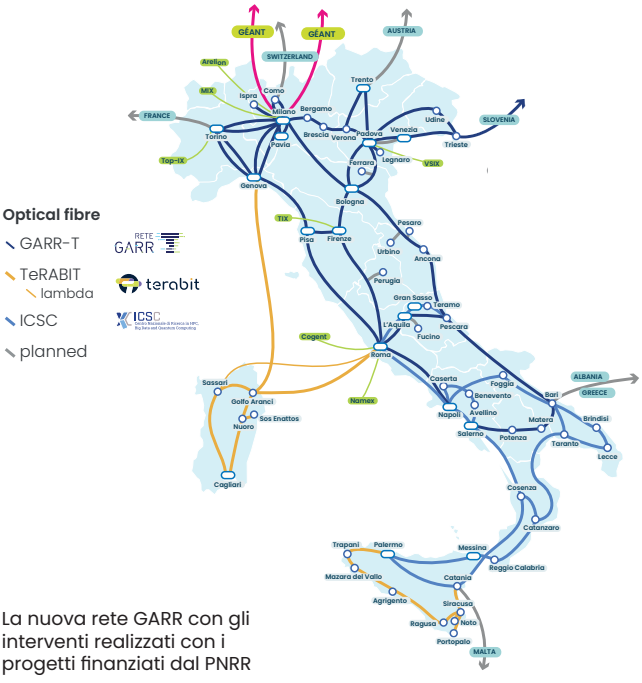
Un'infrastruttura digitale che cambia il Paese

Il contributo congiunto dei progetti TeRABIT e ICSC ha permesso la creazione di un sistema nazionale integrato, in cui rete, calcolo e gestione dei dati operano in modo coordinato. I risultati sono tangibili: la capacità della dorsale è cresciuta fino a circa 36 Terabit al secondo e la rete nazionale è stata completamente rinnovata nelle sue componenti ottiche e di trasporto, con particolare attenzione alle regioni del Mezzogiorno, dove la migrazione è stata completata al 100% nel 2025, con l'infrastruttura di Sicilia, Campania, Puglia e Calabria completamente integrata nella rete GARR-T.

Il progetto GARR-T ha inoltre consentito l'introduzione dello **spectrum sharing** e la realizzazione di collegamenti diretti a capacità molto elevate, come il link diretto a 1,6 Tbps tra CERN e CNAF con delay sotto i 10 ms, in grado di garantire la capacità necessaria a supporto del calcolo dei nuovi esperimenti LHC previsti nei prossimi anni.

Questo modello favorisce la **competitività scientifica del Paese**, consente un utilizzo più equo delle risorse e migliora l'accesso ai servizi avanzati anche in aree tradizionalmente meno infrastrutturate.

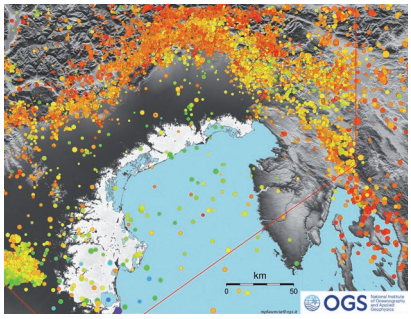
L'impatto è già visibile in diversi ambiti applicativi. Tra questi, riveste particolare interesse lo **sviluppo dell'urgent computing**, che consente di generare rapidamente simulazioni e analisi utili alle autorità competenti. Nel progetto UrgentShake, ad esempio, l'elaborazione in tempo quasi



La nuova rete GARR con gli interventi realizzati con i progetti finanziati dal PNRR

reale di modelli sismici è stata resa possibile proprio grazie alla combinazione tra rete ad alta capacità e supercalcolo avanzato, riducendo i tempi di calcolo da diverse ore a pochi minuti e fornendo alla Protezione Civile strumenti concreti per la gestione delle emergenze.
GARR ha svolto un ruolo centrale nei progetti TeRABIT e ICSC, costruendo un'infrastruttura digitale nazionale che posiziona l'Italia ai vertici europei. Questo sistema integrato di rete, calcolo e dati rafforza la competitività scientifica del Paese, abilita nuove frontiere di ricerca e aumenta la capacità di attrarre investimenti e partecipare a collaborazioni internazionali di eccellenza.

- terabit-project.it
- supercomputing-icsc.it

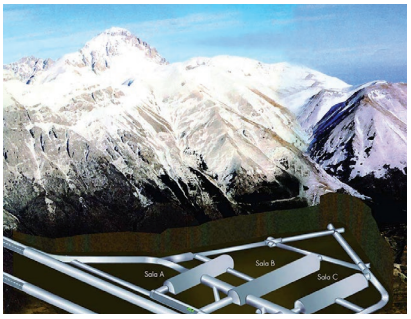


UrgentShake: simulazioni sismiche in tempo quasi reale

UrgentShake è un sistema sviluppato dall'OGS nell'ambito dell'ecosistema Terabit, con il supporto tecnico di CINECA, al quale ora contribuiscono anche alcune università italiane. Ha l'obiettivo di generare simulazioni sismiche in tempo quasi reale, fornendo alla Protezione Civile e alle autorità competenti uno strumento avanzato per supportare le valutazioni immediate successive a un evento tellurico.

Grazie all'integrazione tra la rete ad altissima capacità di GARR e le risorse di supercalcolo di Terabit (HPC Cineca e HPC Bubble INFN), UrgentShake riduce i tempi di elaborazione tradizionali da molte ore o giorni a minuti o poche ore, fornendo scenari del moto del suolo con livelli di dettaglio progressivamente crescenti, utili per la gestione delle diverse fasi dell'emergenza.
Si tratta di uno dei casi d'uso più significativi dell'articolazione tra rete, HPC e Big Data abilitate dal PNRR, con un impatto diretto sulla sicurezza pubblica e sulla capacità del Paese di rispondere in modo tempestivo a eventi critici.

Vedi la presentazione di Davide Salomoni al Workshop GARR 2025 sulle prossime sfide del Centro Nazionale



LNGS: dal nuovo Centro HPC all'arrivo di GARR-T

Ai Laboratori Nazionali del Gran Sasso è in corso la realizzazione di un nuovo centro HPC nell'ambito del progetto ICSC, con lo scopo di aumentare la resilienza del Paese nel caso di disastri naturali ed antropici. Il centro si sviluppa attorno a risorse dismesse da CINECA negli ultimi anni, integrato da nuovi sistemi HPC dotati di GPU e storage ad alte prestazioni acquisiti dal progetto. Il potenziamento della connettività grazie a due nuovi PoP GARR-T, operativi a collegamenti multipli 100 Gbps, consentirà di integrare in modo più efficace le attività del laboratorio con l'ecosistema nazionale del supercalcolo, ampliando le possibilità di ricerca e collaborazione.

La rivoluzione digitale della Sardegna

L'intervento realizzato attraverso TeRABIT ha inserito la Sardegna in una posizione centrale all'interno della rete nazionale della ricerca. L'anello in fibra ottica terrestre di circa 1.100 chilometri, l'acquisizione di spettro ottico su due sistemi sottomarini, la realizzazione di collegamenti sottomarini con capacità iniziale (day 0) di 1,6 Tbps verso la dorsale nazionale, garantiscono oggi all'isola condizioni infrastrutturali equivalenti a quelle del continente, con rilevanti ricadute scientifiche e territoriali.

Dopo il PNRR: le prospettive del Centro Nazionale ICSC

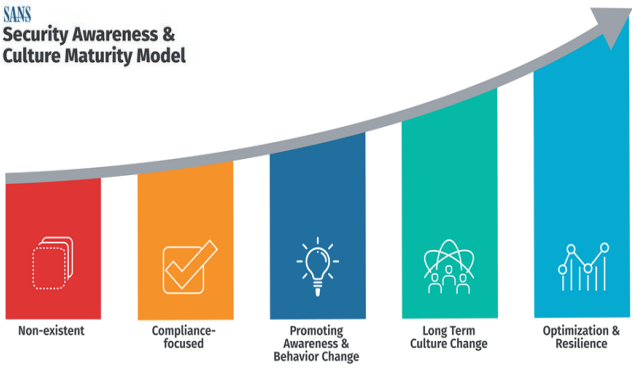
Con la conclusione delle attività PNRR, il Centro Nazionale ICSC avvia una nuova fase dedicata al consolidamento dell'infrastruttura nazionale di supercalcolo, Big Data e tecnologie quantistiche.
Le priorità riguardano il rafforzamento della capacità computazionale e l'evoluzione dei servizi per l'intelligenza artificiale, in continuità con le nuove iniziative europee, tra cui lo sviluppo della AI Factory italiana, a cui ICSC partecipa (bando di gara pubblico e piano operativo definito, in fase di realizzazione) e la prospettiva delle AI Gigafactory continentali, cinque in totale e finanziate al 50% dalla Commissione europea e al 50% dai privati; si tratta di un progetto complesso, per il quale l'Italia si sta candidando e che richiede investimenti dell'ordine di circa 5 miliardi di euro.
ICSC è inoltre diventato nodo della Federazione EOSC, ampliando il proprio ruolo nella condivisione e gestione dei dati della ricerca a livello europeo.

Security Awareness Boost

Come lo studio del comportamento e delle reazioni negli esseri umani cambiano e potenziano il modo di fare security awareness

di Simona Venuti

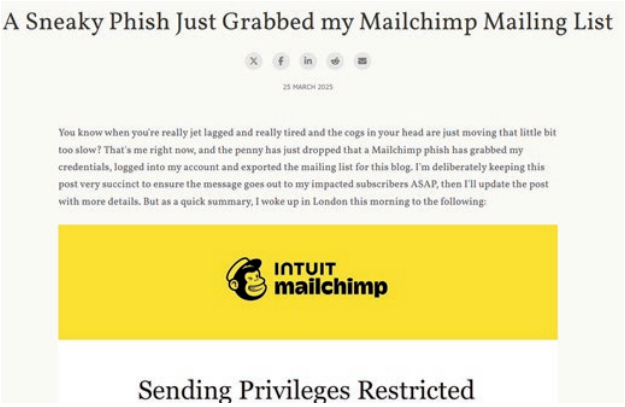
Come tutti sappiamo, si è concluso da poco il CyberSecurity Awareness Month, una iniziativa promossa dall'agenzia europea ENISA che consiste nel dedicare un mese dell'anno, ottobre, ad iniziative e campagne di informazione e sensibilizzazione volte a migliorare la consapevolezza della sicurezza nell'utilizzo dei dispositivi digitali. L'occasione è buona per raccontare un po' di come è cambiato negli ultimi anni il modo di fare awareness, alla luce di studi sul comportamento e reazioni umane.
Ciascuna organizzazione è impegnata quasi quotidianamente nel fornire al proprio personale corsi e strumenti di formazione all'awareness durante tutto il periodo dell'anno, ma questo tipo di formazione non è così banale come potrebbe sembrare. Non si tratta solo di "insegnare a riconoscere un link fasullo o una mail di SPAM": questo è il livello del minimo indispensabile per formazione all'awareness, il livello "compliance-focus", come si può vedere nel modello SANS Security Awareness & Culture Maturity Model.
Ciò che invece dovremmo perseguire nel fornire questo tipo di formazione sono i passi successivi, cioè una specie di "crescita interiore", in cui ciascuno di noi sappia di **essere veramente in prima linea nella difesa delle nostre organizzazioni!**
Ma per diventare un difensore efficace non è sufficiente sapere cosa non cliccare, è necessario introdurre e coltivare buone e sicure abitudini, attraverso sistemi di cambiamento del comportamento, e successivamente promuovere nell'organizzazione una cultura aziendale alla sicurezza in cui la sicurezza non è soltanto un processo (o non si trova soltanto nei processi), ma è un valore imprescindibile dell'organizzazione, in perfetta armonia con tutto il resto.
Come scrivo ogni volta, e ogni volta purtroppo è sempre vero, il mondo là fuori pullula di criminali e truffatori che utilizzano tecniche di social engineering e phishing per carpire dati, accessi, informazioni da utilizzare per i propri attacchi, e diventano sempre più sofisticati, minacciosi e pericolosi.
L'ultima (brutta) tendenza è lo sfruttamento pesante dell'intelligenza artificiale nel creare falsi indistinguibili dal vero,



e questo si applica a video, messaggi audio (qualcuno avrà ricevuto su WhatsApp un presunto audio del figlio/a che chiede aiuto e soldi, sono praticamente perfetti!), ai bot online che sono più numerosi delle persone "vere", utilizzati per SCAM sia per proporre truffe crypto che per impersonare persone che lentamente vengono catturate dal nostro fascino irresistibile e si "innamorano" di noi, alla perfezione con cui una AI può scrivere un documento o un testo usando lo stile del Direttore Generale... tutto ciò eleva di molti ordini di grandezza la possibilità di sfruttare le debolezze di noi poveri esseri umani e lavoratori.
In questo clima di pericolo, nell'ottica di raggiungere nel lungo termine l'armonia precedentemente accennata, dovremmo ripensare ai modi in cui conduciamo le nostre campagne, anche alla luce di nuovi contributi e studi in relazione ai comportamenti e reazioni umani, e come possiamo essere allenati per essere più impenetrabili.

Sfatare un mito: il personale non tecnico non è "l'anello debole della catena".

È vero che nel 68% delle volte un breach inizia con un phishing (fonte: Rapporto Verizon 2024), ma le vittime non sono soltanto fra il personale non tecnico: in molti casi la vittima è un membro del board, e spesso è personale tecnico, specializzato anche in sicurezza informatica.
Ci sono due esempi recenti e famosi di personale tecnico altamente competente che è caduto in una banale mail di phishing. Lo scorso agosto c'è stato **uno dei più grandi incidenti di sicurezza** mai avvenuti nella storia: è stato compromesso l'account di uno degli sviluppatori delle librerie NPM (Qix, aka Josh Junon) ed è stato inserito del codice malevolo nei sorgenti delle librerie, che sono utilizzate da milioni di computer e server nel mondo! In pochi minuti, grazie ad aggiornamenti automatici, si sono infettati centinaia di migliaia di sistemi, provocando uno dei più grandi incidenti alla supply chain.
L'account dello sviluppatore, che è una persona estremamente competente e sensibile alla sicurezza, è stato compromesso attraverso una mail di phishing con un link ad una pagina fasulla di GitHub, in cui l'ignaro ha inserito le proprie credenziali github, dove risiede il codice sorgente delle librerie.
In aprile il famosissimo esperto di sicurezza informatica Troy Hunt, colui che ha inventato il sito Have I Been Pwned,



ha subito il furto di tutta una mailing list, a seguito della compromissione del suo account... attraverso una "stupida" mail di phishing!
Questi esempi ci fanno chiaramente capire che il problema non è di conoscere quando una mail è farlocca o un link non è un link al sito ufficiale, entrambi conoscevano benissimo queste tecniche di riconoscimento del phishing. Entrambi però affermano che "erano stanchi, avevano jet lag, stavano pensando ad altre mille cose contemporaneamente, erano troppo carichi di lavoro"; che insomma, erano occupati con la mente a fare altro, e la mano è stata più veloce del pensiero.
Tutto questo significa che **non è il personale non tecnico ad essere l'anello debole della catena**: siamo tutti noi esseri umani che siamo fatti così, siamo per natura e soprattutto per abitudine, vulnerabili a certe reazioni inconsce, come i campanellini di Pavlov: "vedi link – clicca".
Significativi a questo proposito sono due studi, che sfatano un altro mito: *Phishing in Organizations: Findings from a Large-Scale and Long-Term Study*, pubblicato su IEEE Symposium on Security and Privacy 2022 e *Understanding the Efficacy of Phishing Training in Practice*, pubblicato su IEEE Symposium on Security and Privacy 2025.

Sfatare un altro mito: le simulazioni di phishing

I risultati di un esperimento del primo studio ci dicono che somministrando simulazioni di phishing a personale non tecnico è vero che solo una piccola parte cade nel presunto phishing, ma sono molti di più gli svantaggi dei benefici: più volte viene somministrato il test e meno diventa efficace (più persone cadono nel phishing ai test successivi), il personale si sente sempre sul banco di prova, diminuisce la fiducia nel datore di lavoro (mi fa le trappole perché non si fida di me), aumento dell'ansia ogni volta che arriva una mail che potrebbe essere un test. Siamo veramente sicuri che una simulazione di phishing rispetti i principi del Belmond Report?
In pratica è come mettere una pentola bollente davanti ad un bambino per insegnargli a non toccare le pentole bollenti. O lasciar cadere 10 euro in corridoio con una telecamera per vedere chi li raccoglie.
E infine: cosa fare delle persone che cadono nel phishing?

Facciamo fare un corso soltanto per loro, mettendole alla gogna, oppure facciamo fare un corso "di recupero" a tutti, alimentando risentimento e frustrazione nei colleghi che hanno passato il test?
Lo studio prosegue elencando alcune **alternative** che risultano migliori rispetto alle simulazioni di phishing, come ad esempio quelle riportate di seguito.
Bottone per la segnalazione. Inserire nel client di posta un bottone "Segnala mail phishing". Attraverso il bottone chiunque abbia il sospetto che una mail non sia buona, può segnalarla ai tecnici, che la valuteranno. In questo modo non c'è nessuna ansia all'arrivo delle mail. Inoltre questo sistema ci fa sentire parte di coloro che contribuiscono al benessere dell'organizzazione, ci fa sentire considerati e approvati. Ci sentiamo utili.
Simulazioni come gioco. Usare simulazioni di phishing ma in modo aperto e non all'insaputa del personale, come gioco di gruppo. Utilizzare il prodotto come un gioco di gruppo: vince chi scopre per primo un phishing o chi ne individua di più. Possiamo stimolare le persone a creare dei phishing per indurre i propri colleghi a cascarci, possiamo inventare giochi di ruolo basati sul social engineering.

Concludendo: perché cadiamo in un phishing?
Come ci raccontano Qix e Troy Hunt, oltre a cattive abitudini da cambiare e cultura da coltivare, quello che ci fa cadere è stress, stanchezza, disattenzione, multitasking, pensieri altrove; clicchiamo per abitudine come un riflesso istintivo.

Mantenere la mente sgombra, libera, in pace, ed essere presenti a sé stessi sul momento, aiuta a prendere coscienza del click e non ci fa cadere nel phishing

Se tutti indistintamente siamo vulnerabili, non è una colpa!

- È una caratteristica dell'essere umano
- Un'abitudine da cambiare
discipline di Behaviour Changing
- Una cultura da coltivare
discipline di Security Culture

Cadere nel phishing quindi non dipende perlopiù dal dipendente, ma per esempio dal momento della giornata, dalle cose che stiamo facendo in quel momento, dall'umore che abbiamo, da quanto abbiamo dormito, dai pensieri che ci passano per la testa.
Per aiutarci ad essere più presenti, un approccio utile potrebbe essere quello della **Mindfulness**, dell'auto-consapevolezza. Le ultime ricerche nel campo della psicologia del phishing sono arrivate alla conclusione che mantenere la mente sgombra, libera, in pace, ed essere presenti a sé stessi sul momento, aiuta a prendere coscienza del "click" e non ci fa cadere nel phishing.
Anna Collard, esperta in CyberPsichology, studia proprio la disciplina della mindfulness in awareness. Arriva una mail sospetta? Alza gli occhi, guarda fuori, fai due passi, annaffia una pianta, accarezza il gatto. **Fai qualcosa che ti liberi la mente** e quando tornerai a quella mail sarai presente solo a quella mail, con consapevolezza e attenzione. A mente libera, senza impazienza e senza farsi sovrastare dalle cose che incombono, è più difficile farsi fregare.
Questo è uno dei motivi per cui la campagna per il CyberSecurity Month di Geant quest'anno è stata incentrata su "Be Mindful, Stay Safe".

• security.geant.org/cybersecurity-campaign-2025

Dai Security Days ai gruppi di lavoro

Formazione NIS2 e collaborazione nella comunità GARR

di Marta Mieli, Alessandro Inzerilli e Leonardo Lanzi

L'evoluzione delle minacce informatiche e la crescente dipendenza dalle infrastrutture digitali rendono indispensabile un rafforzamento delle misure di sicurezza. Le direttive europee, culminate nella **NIS2**, mirano a garantire la continuità dei servizi essenziali e a sostenere un livello elevato di resilienza digitale. In questo quadro, GARR è chiamato non soltanto ad assicurare la conformità alla normativa, ma anche a svolgere un ruolo chiave nel supportare l'intera comunità verso modelli collaborativi, pratiche condivise e soluzioni comuni.

I **Security Days** hanno rappresentato per la comunità dell'università e della ricerca **un momento di confronto senza precedenti sui temi della sicurezza informatica**. Per la prima volta l'evento si è svolto nella forma di un workshop dedicato, pensato non solo come occasione di aggiornamento tecnico, ma come spazio di dialogo strutturato tra le diverse componenti della comunità GARR: responsabili ICT, esperti di sicurezza, personale tecnico-amministrativo e decisori.

La richiesta di partecipazione è stata superiore alle aspettative e non è stato semplice per il comitato di programma condensare in appena due giornate la ricchezza di contributi, esperienze e sollecitazioni emerse negli ultimi anni. Il risultato è stato un **programma intenso**, articolato in 9 sessioni plenarie e 26 sessioni parallele, nel corso delle quali sono stati affrontati temi centrali per la cybersecurity: dall'impatto e dall'implementazione della nuova direttiva NIS2 alla gestione degli incidenti, dalla sicurezza della supply chain all'identità federata, dall'autenticazione multifattore alle attività di vulnerability assessment, fino a DNSSEC e alla creazione di uno CSIRT, formazione e strumenti open accessibili in ambito federato.

Tra i temi che hanno catalizzato maggiore attenzione e stimolato un confronto trasversale durante l'intero evento, la **normativa NIS2** ha occupato un ruolo centrale. Il decreto legislativo n. 138 del 2024, che ha recepito in Italia la Direttiva (UE) 2022/2555, nota come NIS2, introduce infatti un quadro profondamente rinnovato per la sicurezza delle reti e dei sistemi informativi, con l'obiettivo di garantire un livello elevato e uniforme di resilienza digitale in tutti gli Stati membri. Per la comunità GARR, composta in larga parte da enti provenienti dal mondo dell'istruzione e della ricerca, l'impatto è particolarmente rilevante: la maggior parte delle organizzazioni collegate alla rete GARR rientra ora esplicitamente nell'ambito di applicazione della normativa.

Un passaggio chiave del nuovo quadro regolatorio è rappresentato dalle cosiddette "specifiche di base", adottate dall'Agenzia per la Cybersicurezza Nazionale con la determinazione del 14 aprile 2025. Esse definiscono le misure

minime di sicurezza che le organizzazioni soggette alla NIS devono adottare entro ottobre 2026, nonché le tipologie di incidenti per le quali, da gennaio 2026, scatterà l'obbligo di notifica al CSIRT Italia. Proprio a queste specifiche è stata dedicata la presentazione "NIS2: indicazioni operative per la comunità", curata da **Alessandro Inzerilli** (Security compliance e risk manager di GARR), con l'obiettivo di fornire una lettura concreta degli adempimenti richiesti e di offrire prime indicazioni pratiche per la loro interpretazione e implementazione.

La presentazione ha suscitato un interesse tale da rendere evidente l'esigenza di un approfondimento ulteriore. In collaborazione con l'ufficio formazione GARR, si è quindi deciso di trasformare questi contenuti in un corso strutturato, erogato in modalità webinar attraverso la piattaforma Learning GARR. Il **webinar**, che si è tenuto il 4 dicembre, ha registrato quasi 500 iscritti sulla piattaforma e una partecipazione complessiva, tra diretta e visualizzazioni successive, di oltre 1.500 utenti unici, grazie alla trasmissione simultanea su GARR TV, YouTube, LinkedIn e Facebook.

Nel corso di oltre un'ora e mezza, il webinar ha delineato innanzitutto il quadro normativo europeo e nazionale, chiarendo ambiti di applicazione, soggetti coinvolti e distinzione tra soggetti essenziali e importanti. Ampio spazio è stato dedicato agli obblighi in capo agli organi di amministrazione e direttivi, chiamati a svolgere un ruolo attivo e non delegabile nella gestione del rischio cyber e nella supervisione delle misure adottate. La seconda parte si è concentrata sulle specifiche di base, illustrate nei loro criteri di progettazione, derivati dal Framework Nazionale per la Cybersecurity e la Data Protection e nei loro contenuti: 116 requisiti per i soggetti essenziali e 87 per quelli importanti, in larga parte di natura organizzativa. Audit, ruoli e responsabilità, gestione degli asset, continuità operativa, gestione delle crisi, formazione del personale e sicurezza della supply chain sono solo alcuni degli ambiti affrontati, accanto ai requisiti tecnologici relativi a monitoraggio, protezione delle reti, gestione delle vulnerabilità e controllo degli accessi.

Particolare attenzione è stata riservata al **processo di gestione e classificazione degli incidenti**, destinato a diventare il primo obbligo operativo già a partire dal 2026. In questo contesto sono stati forniti riferimenti a standard e framework internazionali e indicazioni utili per impostare un percorso di adeguamento coerente e sostenibile. Il webinar ha inoltre segnato l'avvio di un **ciclo formativo** più ampio, denominato **Security Date**, pensato per rispondere in modo continuativo ai fabbisogni formativi emersi dalla comunità: un appuntamento al mese per tutto il 2026, affiancato da corsi in presenza in occasione dei principali eventi GARR.

Accanto alla dimensione formativa, i Security Days hanno fatto emergere con chiarezza un'altra esigenza: quella di rafforzare il coordinamento e la collaborazione operativa tra gli enti della comunità. L'interesse verso la sicurezza informatica è cresciuto in modo esponenziale negli ultimi anni, anche in conseguenza dei cambiamenti introdotti dalla pandemia, che hanno ampliato le superfici di attacco e reso più complesse le dinamiche del cybercrime. In questo scenario, è sempre più evidente che la risposta non può essere solo individuale, ma deve basarsi su un impegno condiviso, su strumenti comuni e su una visione di sistema.

La risposta agli attacchi informatici non può essere solo individuale, ma deve basarsi su un impegno condiviso, su strumenti comuni e su una visione di sistema

Durante i momenti di confronto, è emersa più volte l'aspettativa che **GARR possa svolgere un ruolo di facilitatore e coordinatore, mettendo a disposizione servizi, piattaforme e linee guida comuni**: dalla gestione e prevenzione degli incidenti, a strumenti uniformi per il risk assessment e la governance, fino alla formazione specialistica. Per dare una risposta strutturata a queste richieste, è stata proposta la **creazione di gruppi di lavoro tematici,** individuati attraverso un sondaggio rivolto ai partecipanti ai Security Days e aperto anche al coinvolgimento di ulteriori colleghi all'interno delle organizzazioni.

Il sondaggio ha permesso di individuare le aree ritenute prioritarie. In testa si sono collocati il **risk assessment, la gestione degli incidenti e i tools di sicurezza,** seguiti dalla **governance** e **compliance**, comunque valutata come altamente rilevante. Considerando anche le sovrapposizioni naturali tra alcuni ambiti, la proposta emersa è stata quella di avviare inizialmente due gruppi di lavoro: uno dedicato alla Gestione degli incidenti e tools di sicurezza, l'altro focalizzato su Governance e gestione del rischio.

Il **primo gruppo** avrà come obiettivo l'analisi e la possibile realizzazione di un punto di accesso condiviso e multitenant, basato su modelli di accesso per ruolo e integrato con l'infrastruttura di identità federata IDEM, nonché l'integrazione di strumenti per la gestione degli incidenti, la condivisione delle informazioni e la cyber threat intelligence in un'unica piattaforma. Il **secondo gruppo** lavorerà invece sull'individuazione di strumenti comuni per il risk assessment, sulla definizione di approcci condivisi alla gestione del rischio nella comunità GARR e su modelli efficaci di gestione documentale della compliance normativa, evitando soluzioni meramente formali.

GARR sta attualmente lavorando alla redazione dei charter dei due gruppi, che ne definiranno scopo, obiettivi, tempistiche, ruoli e modalità operative. Il passo successivo sarà l'organizzazione di un primo incontro, per discutere e finalizzare le bozze e avviare ufficialmente le attività. L'obiettivo, ambizioso ma concreto, è quello di produrre risultati tangibili già nel corso del 2026, da condividere con l'intera comunità, possibilmente in occasione dei prossimi GARR Security Days previsti per il prossimo autunno.

In questo senso, i Security Days non rappresentano un punto di arrivo, ma l'**inizio di un percorso**. Un percorso che unisce formazione, collaborazione e condivisione di competenze, e che mira a rafforzare in modo strutturato la resilienza digitale della comunità GARR, trasformando gli obblighi normativi e le sfide di sicurezza in un'opportunità di crescita collettiva.

• securitydays25.garr.it

EOSC entra nella fase operativa

Al via la Federazione di nodi EOSC Europe al Symposium 2025

L'Italia protagonista con due nodi attivi nella nuova infrastruttura che collegherà dati, servizi e comunità di ricerca in tutta Europa

di Sara Di Giorgio

L'EOSC Symposium 2025, svoltosi a Bruxelles dal 3 al 5 novembre, ha rappresentato un passaggio cruciale per l'attuazione della European Open Science Cloud (EOSC) e per l'avvio operativo della **EOSC Node Federation**, una nuova infrastruttura destinata a federare dati, servizi e risorse digitali per la ricerca in Europa.

L'evento, promosso dall'EOSC Association con il sostegno della Commissione europea, ha riunito circa 500 rappresentanti del mondo della ricerca, delle istituzioni e delle infrastrutture digitali, sottolineando la volontà di proseguire con determinazione verso un ecosistema federato realmente operativo e sostenibile.

Durante la sessione inaugurale, **Marc Lemaître**, Direttore Generale della DG Research & Innovation, ha delineato il quadro politico e strategico della federazione, ribadendo il ruolo centrale dell'Europa nella gestione dei dati scientifici e nella cooperazione internazionale: "Dobbiamo agire insieme per completare velocemente la federazione e farne la spina dorsale dell'ecosistema digitale della ricerca e dell'innovazione europea."

Il successivo intervento di **Robbert Dijkgraaf**, Presidente eletto dell'International Science Council, ha ampliato la prospettiva al contesto globale, sottolineando come la gestione integrata dei dati e delle infrastrutture digitali sia ormai essenziale per affrontare le grandi sfide della scienza contemporanea, dal cambiamento climatico alla salute pubblica.

Due nodi italiani tra i primi tredici della Federazione EOSC

L'Italia si è distinta come **unico paese europeo con due nodi attivi** nella prima fase di costruzione della federazione, selezionati nel febbraio 2025 dopo un processo competitivo di sei mesi che ha coinvolto oltre 100 candidature. Tra i **13 nodi selezionati in Europa**, l'Italia è rappresentata dal nodo nazionale **ICSC**, il Centro nazionale di ricerca in High Performance Computing, Big Data and Quantum Computing, designato come EOSC National Node | Italy, e dal nodo tematico **Blue-Cloud**, dedicato alla scienza marina e coordinato dal Consiglio Nazionale delle Ricerche.

La candidatura e la creazione del nodo nazionale ICSC sono state possibili grazie al supporto dell'intera comunità italiana ed in particolare dai membri di **ICDI (Italian**

Computing and Data Infrastructure), l'iniziativa nazionale per l'Open Science Cloud guidata da GARR, che ne rappresenta l'Italia all'interno della EOSC Association come "mandated organisation". ICDI riunisce esperti provenienti dalle principali infrastrutture di ricerca e digitali italiane, promuovendo la transizione verso la Scienza Aperta e l'applicazione dei principi FAIR. Tra l'altro attraverso il centro di competenza di ICDI, GARR ha coordinato anche il progetto europeo Skills4EOSC, recentemente concluso e diventato un punto di riferimento per le attività di training e per l'upskilling dei ricercatori nella Federazione EOSC.
Il nodo nazionale ICSC offre un **catalogo iniziale di servizi** messi a disposizione dalla comunità di ICDI, infrastrutture di calcolo e servizi avanzati per la ricerca, sviluppando flussi di lavoro federati per l'analisi di grandi dataset. Il nodo tematico Blue-Cloud, invece, evolve verso un ecosistema federato per la **Digital Twin of the Ocean**, mettendo a disposizione Virtual Research Environments, servizi di calcolo e strumenti analitici per la ricerca oceanografica e la blue economy.

I tre use case che mostrano il potenziale della Federazione EOSC

Uno dei momenti più attesi del Symposium è stato l'intervento dei coordinatori dei **tre casi d'uso scientifici cross-node**, che hanno offerto alla comunità una prima dimostrazione operativa di una rete federata di dati e servizi FAIR.
Durante la presentazione è stato mostrato in tempo reale come un ricercatore possa utilizzare la Federazione EOSC. Grazie a un unico punto di accesso e all'infrastruttura federata di autenticazione e autorizzazione, è possibile muoversi agevolmente tra i repository di dati dei diversi nodi, sfruttando servizi di calcolo, strumenti di intelligenza artificiale e risorse analitiche condivise. **Giovanni Guerrieri** del CERN ha illustrato come sia possibile "ri-creare" una grande scoperta di fisica delle particelle combinando dati storici e potenza di calcolo distribuita. **Björn Grüning** di Galaxy Europe/Università di Friburgo ha mostrato come enormi dataset di immagini possano essere elaborati attraverso workflow riutilizzabili per affrontare sfide scientifiche in astrofisica, clima e scienze marine. Infine, **Andreas Türk** di BBMRI-ERIC ha evidenziato come modelli diagnostici basati su intelligenza artificiale, validati in un ospedale, possano essere applicati in tempo reale a immagini provenienti da un altro ospedale, garantendo sicurezza e interoperabilità. Questi esempi dimostrano chiaramente come la Federazione EOSC possa abilitare una ricerca collaborativa, trasparente e riproducibile, trasformando il modo in cui la scienza europea affronta le proprie sfide.
Il nodo italiano ICSC ha fornito un contributo essenziale a due use case: quello del CERN sui workflow di analisi distribuita e quello BBMRI-ERIC sullo studio di immagini mediche, dove il contributo del nodo italiano è stato fondamentale.

Una tappa chiave per l'Europa della Scienza Aperta

Un momento simbolico del Symposium è stata la firma del Memorandum of Understanding (MoU) tra la EOSC Association e i rappresentanti dei primi nodi candidati alla federazione, che ha sancito l'avvio formale della fase operativa della EOSC Federation. Durante la seconda giornata, i lavori si sono concentrati sulla governance dei nodi, sull'allineamento tecnico e sull'avvio della call per la seconda ondata di nodi (prevista per la primavera 2026), che sarà sostenuta da un **finanziamento complessivo di 1,6 milioni di euro**, erogato tramite cascading grants attraverso il progetto EOSC Gravity.
Nel corso dei tre giorni di lavoro, il Symposium ha offerto un confronto ampio e dinamico sul ruolo centrale di EOSC nella trasformazione digitale del sistema europeo della ricerca. Le sessioni plenarie e parallele hanno affrontato temi chiave come la costruzione di un ambiente di fiducia, sicuro e sovrano per i dati e i servizi FAIR, la valorizzazione delle iniziative nazionali che accelerano l'attuazione di EOSC e la definizione di nuovi incentivi per favorire la partecipazione dei ricercatori e l'apertura verso innovatori, start-up e imprenditori accademici. Ampio spazio è stato dedicato anche alla formazione e allo sviluppo delle competenze necessarie per operare in un contesto di Scienza Aperta, con particolare attenzione ai ruoli emergenti dei data steward e del personale di supporto alla ricerca.
In sintesi, il Symposium 2025 ha dato una prova concreta che la European Open Science Cloud rappresenta uno dei pilastri della futura infrastruttura scientifica europea. Come indicato nel **rapporto Heitor** sulla competitività europea, l'EOSC ha il potenziale per diventare l'infrastruttura più ampiamente utilizzata in Europa, se sviluppata nel modo giusto. I risultati presentati a Bruxelles mostrano che l'Europa sta effettivamente percorrendo questa strada e che l'Italia, con la sua partecipazione attiva, è parte integrante e gioca un ruolo di spicco in questo processo di crescita e cooperazione scientifica.
Il percorso proseguirà nel 2026, con la fase di entrata in produzione formale dei nodi, consolidando ulteriormente la rete europea.

• eosc.eu/eosc-symposium-2025

Che cos'è l'EOSC?

Il Cloud Europeo per la Scienza Aperta (EOSC), lanciato nel 2018 dalla Commissione europea, facilita l'accesso e il riutilizzo dei dati della ricerca, promuovendo una scienza basata sui dati sicura e interoperabile. EOSC è coordinato dall'EOSC Association, che gestisce un accordo di partenariato con la Commissione, condiviso anche da Stati Membri e Paesi associati a Horizon Europe. EOSC mira a creare un'infrastruttura digitale federata composta da Nodi, Nodi Tematici e Nodi Nazionali, basata sui principi FAIR (Findable, Accessible, Interoperable, Reusable) della Scienza Aperta, rafforzando al contempo la sovranità dei dati europei e la competitività del continente nell'economia globale della conoscenza.

• eosc.eu
• open-science-cloud.ec.europa.eu

Skills4EOSC: l'ecosistema europeo delle competenze in open science

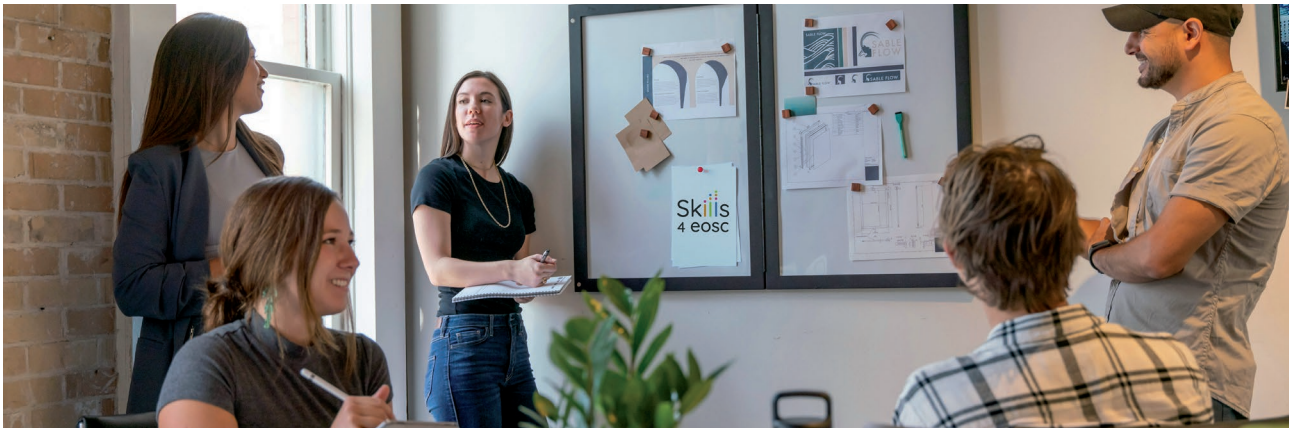
Metodologie, formazione e reti: l'eredità del progetto che in tre anni di lavoro ha rafforzato le competenze EOSC

di Sara Di Giorgio

Ad agosto 2025 si è chiuso Skills4EOSC, il progetto europeo coordinato da GARR che, per tre anni, ha lavorato per trasformare l'Open Science in una pratica diffusa e sostenibile in tutta Europa. Partito a settembre 2022 con 46 partner provenienti da 18 paesi, il progetto ha realizzato una rete europea di Competence Centres, in grado di supportare un ecosistema condiviso per sviluppare competenze, definire profili professionali, costruire curricula e produrre risorse formative a sostegno della scienza aperta e dell'European Open Science Cloud (EOSC).
In questi tre anni, Skills4EOSC ha prodotto strumenti concreti e ampiamente adottati dalle comunità della ricerca, dalle infrastrutture scientifiche, dalle università e dalle amministrazioni pubbliche. Il progetto, per prima cosa, ha sviluppato una metodologia europea per definire i profili e le competenze essenziali dell'Open Science, nota come Minimum Viable Skills Set (MVS), e un approccio FAIR-by-Design per la creazione di risorse formative aperte, riutilizzabili e di qualità. Sulla base dei curricula individuati dagli MVS, sono stati poi realizzati corsi di formazione progettati con la metodologia FAIR-by-Design, che ne facilitano il riuso e la ricercabilità. I formatori selezionati dai Competence Centres del Network hanno seguito un programma formativo dedicato, impegnandosi a loro volta di replicare i corsi nelle comunità nazionali dei ricercatori, adattando e riutilizzando i materiali di Skills4EOSC. Infatti tutti i corsi realizzati sono liberamente accessibili e scaricabili sulla piattaforma di e-learning di Skills4EOSC.
Grazie a queste attività, il progetto ha creato e consolidato un network europeo di Competence Centres in grado di garantire la sostenibilità e l'allineamento dei risultati nel lungo periodo, assicurando che le competenze e le risorse generate continuino a supportare la diffusione e l'implementazione dell'Open Science in Europa.

Minimum Viable Skillsets: una metodologia europea per i curricula dell'Open Science

Uno dei pilastri di Skills4EOSC è la definizione dei Minimum Viable Skillsets, un framework per identificare un insieme di competenze essenziali per 14 profili chiave per la gestione dei dati FAIR e la progettazione di politiche per l'Open Science. Gli MVS sono stati sviluppati attraverso una metodologia di co-creazione, con consultazioni iterative e feedback da comunità nazionali e internazionali. Ne è nato un catalogo europeo che oggi rappresenta un riferimento per la progettazione dei curricula di data steward, ricercatori, studenti e dottorandi in



diversi contesti formativi e professionali, dall'università alla formazione continua.
A supporto della loro diffusione, il progetto ha pubblicato una serie di booklet pensati per essere facilmente riutilizzati da università, centri di competenza e infrastrutture di ricerca.

FAIR-by-Design: creare risorse formative aperte e riutilizzabili

Per garantire che i materiali per la formazione prodotti fossero davvero aperti, accessibili e riutilizzabili, Skills4EOSC ha messo a punto la metodologia FAIR-by-Design, oggi adottata da numerose comunità della ricerca. La metodologia è accompagnata da un manuale operativo e un corso online (disponibile nella Learning Platform e su Zenodo), con esempi pratici e raccomandazioni su come scegliere le licenze aperte, organizzare i contenuti, adottare il versioning e applicare i metadati necessari per garantire la più ampia riusabilità, accessibilità e sostenibilità dei materiali didattici. Per facilitare l'applicazione del modello, Skills4EOSC ha realizzato anche un **Quality Compass**, un'applicazione open source che guida i formatori nella valutazione della qualità dei propri corsi, con indicatori, suggerimenti e report automatici.

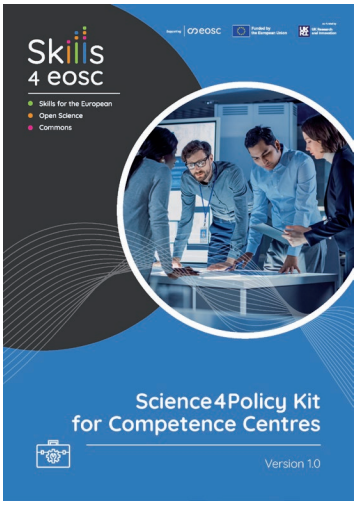
I percorsi formativi di Skills4EOSC

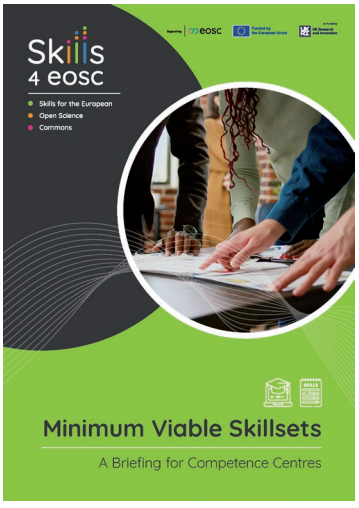
Il programma formativo di Skills4EOSC è uno dei risultati più tangibili del progetto. Tutti i corsi sono liberamente accessibili nella piattaforma di e-learning e i materiali didattici sono stati pubblicati anche su Zenodo. I corsi si rivolgono ai formatori che si occuperanno di organizzare i corsi nelle loro comunità della ricerca (Train-the-Trainer). Nel complesso, sono stati sviluppati **72 corsi**, disponibili in modalità sincrona (durante la durata del progetto), asincrona e self-paced sulla piattaforma, che ha raggiunto 896 utenti registrati, con oltre 900 badge rilasciati.
Tra i principali percorsi formativi, **Science4Policy** è dedicato a funzionari pubblici, policy maker, ricercatori e honest broker con l'obiettivo di rafforzare le competenze necessarie a trasformare l'evidenza scientifica in supporto concreto ai processi decisionali.
La **formazione universitaria** comprende percorsi per studenti e dottorandi, tra cui il corso Open Science Essentials per gli undergraduate e Ticket to Open Science per i PhD, accompagnati da materiali didattici per la modalità di erogazione Train-the-Trainer.
Infine, sono stati realizzati percorsi dedicati alle infrastrutture di ricerca e alle comunità tematiche, sviluppati in collaborazione con EPOS, OPERAS, DiSSCo, ENES e altre iniziative europee, per rispondere alle esigenze specifiche delle diverse discipline scientifiche.
Il progetto ha inoltre pubblicato linee guida, kit e materiali di supporto delle istituzioni, università e centri di competenza nell'erogazione autonoma dei corsi.

Le reti professionali: data steward, bibliotecari e professionisti dell'Open Science

Il lifelong learning è essenziale per mantenere aggiornate le pratiche di gestione dei dati, perché in un contesto in continua evoluzione solo l'apprendimento continuo consente ai professionisti di restare allineati a standard, tecnologie e metodologie sempre nuove. Per supportare questo processo, Skills4EOSC ha rafforzato le reti professionali esistenti e favorito la nascita di nuove comunità. Tra i risultati più significativi figurano la creazione e il consolidamento di **reti di data steward** in diversi paesi e l'attivazione di **25 Open Science Communities** nel network europeo, che hanno sviluppato workshop, materiali formativi e uno starter kit per accompagnare la crescita di nuove reti professionali. Questa rete di comunità offre oggi un terreno fertile per aggiornamento, confronto e innovazione condivisa.
Un importante risultato di questa attività è la creazione, grazie a Skills4EOSC, della **rete dei data steward italiani**, una comunità fondata nel 2022 e oggi in costante crescita, con circa 200 partecipanti. Promossa da enti come l'Università di Bologna e il Politecnico di Torino attraverso il Competence Centre di ICDI, la rete offre uno spazio dedicato allo scambio di conoscenze, al supporto tra pari e alla definizione di buone pratiche, contribuendo a rafforzare il riconoscimento e lo sviluppo professionale dei data steward in Italia.

Scarica le pubblicazioni di Skills4EOSC disponibili liberamente sul sito del progetto





La rete dei Competence Centre: la sostenibilità oltre il progetto

Uno dei traguardi più strategici del progetto è la creazione del **Skills4EOSC Competence Centre Network (CCNet)**, una rete formale di Competence Centre nazionali che garantisce la continuità e la sostenibilità dei risultati nel tempo. Ad oggi la rete conta 11 Competence Centre nazionali che hanno firmato un Memorandum of Understanding impegnandosi ad adottare e aggiornare nel tempo gli output del progetto: curricula, MVS, metodologia FAIR-by-Design, framework per la qualità e la formazione dei formatori.

Il network prevede un modello di governance leggero e flessibile, basato su una presidenza a rotazione e su attività periodiche di coordinamento. ICDI è stato eletto come primo presidente della rete. Sul sito del progetto è stato realizzato anche un **Competence Centre Kit** che raccoglie risorse, template e linee guida per sostenere la nascita di nuovi centri.

Un'eredità che continua

Skills4EOSC ha rappresentato un passaggio fondamentale nella costruzione dell'ecosistema europeo delle competenze per l'Open Science. Grazie a metodologie condivise, percorsi formativi armonizzati e una rete stabile di Competence Centre, il progetto ha posto le basi per rendere l'Open Science "the new normal", come riconosciuto anche dalla SRIA EOSC e dall'EOSC Federation Handbook.

Oggi, gli strumenti e le risorse sviluppate sono pienamente operativi e continueranno a essere aggiornati dalla rete dei Competence Centre e riutilizzati da università, comunità di ricerca, istituzioni pubbliche e infrastrutture scientifiche. Un risultato che conferma il ruolo di GARR nella costruzione di un'Europa più aperta, interoperabile e capace di trasformare i dati della ricerca in valore per la scienza e per la società.

• skills4eosc.eu

FP10: non è ancora finita

di Marco Falzetti
Agenzia per la Promozione della Ricerca Europea (APRE)

Il negoziato sul futuro Programma Quadro europeo per la ricerca e l'innovazione, l'FP10, è entrato in una fase decisiva. Dopo mesi di attesa, discussioni informali e anticipazioni talvolta contraddittorie, la proposta della Commissione europea per il nuovo **Quadro Finanziario Pluriennale (QFP) 2028–2034** ha finalmente delineato un quadro più definito, che tuttavia lascia aperti nodi politici e strategici tutt'altro che marginali. Comprendere oggi lo stato dell'arte significa dunque leggere insieme tre livelli: la visione proposta dalla Commissione, le prime reazioni di Parlamento e Consiglio, e il progressivo convergere delle posizioni della comunità europea della ricerca e dell'innovazione.

Il quadro generale è chiaro: la Commissione ha collocato ricerca e innovazione al centro della strategia economica e sociale europea, riconoscendone il ruolo nella competitività, nella sostenibilità e nell'autonomia strategica dell'Unione. Molti dei timori che circolavano nei mesi precedenti

La Commissione europea ha collocato ricerca e innovazione al centro della strategia economica e sociale europea

– una possibile marginalizzazione della R&I a favore di logiche più industriali o di sicurezza – sembrano dunque scongiurati. Il raddoppio proposto del budget di Horizon, vicino alla soglia simbolica dei 200 miliardi di euro auspicata da diversi contributi autorevoli, rappresenta senza dubbio un segnale politico forte.

Allo stesso tempo, l'architettura complessiva in cui il futuro Horizon si inserisce è cambiata in maniera significativa. Al centro della proposta vi è la creazione dell'**European Competitiveness Fund (ECF)**, destinato a sostenere direttamente la capacità industriale e tecnologica dell'Unione

Il negoziato su FP10 non riguarda soltanto un programma di finanziamento ma il modello di sviluppo che l'Europa intende perseguire in un decennio decisivo

in settori strategici. Ricerca e competitività vengono così ricondotte sotto un quadro più integrato, accompagnato da un unico rulebook, da un rafforzamento degli strumenti di innovazione dirompente e dal tentativo di recuperare terreno nei confronti delle grandi economie globali.
È in questo contesto che si colloca il dibattito più acceso. Se da un lato FP10 conserva esplicitamente autonomia e identità, con un bilancio protetto, dall'altro la relazione operativa tra FP10 ed ECF resta ancora da chiarire. La Commissione ha proposto un coordinamento stretto, fino ad arrivare – almeno nelle prime versioni informali – all'ipotesi di programmi di lavoro integrati. È qui che Parlamento, Consiglio e comunità scientifica si sono mossi in modo concorde nel chiedere di mantenere piena autonomia ai programmi di Horizon, evitando sovrapposizioni che rischierebbero di alterarne la missione originaria: generare conoscenza, promuovere eccellenza, sostenere ricerca collaborativa, creare le condizioni per soluzioni di medio-lungo termine.
È un punto cruciale perché tocca la natura stessa del Programma quadro. La ricerca orientata all'impatto industriale non può essere l'unico paradigma della R&I europea, né tantomeno la lente attraverso cui definire priorità, governance o struttura. La complementarità con ECF è certamente necessaria, ma questa complementarità deve salvaguardare un principio fondamentale: **nell'economia della conoscenza, è la ricerca a trainare l'industria, non viceversa.**
All'interno della proposta, la Commissione conferma in parte la struttura dell'attuale Horizon, rafforza gli strumenti più apprezzati (ERC, MSCA, EIC), valorizza la ricerca collaborativa e introduce elementi di discontinuità rilevanti, come i **programmi problem-oriented** e i **nuovi moonshots**, iniziative ad ampio spettro che dovrebbero combinare fondi europei e nazionali per affrontare sfide strategiche. Si tratta di innovazioni potenzialmente importanti, che però richiedono maggiore chiarezza su governance, obiettivi e collocazione formale: sorprende infatti che i moonshots non compaiano nella parte giuridicamente vincolante della proposta legislativa.
Accanto agli elementi di continuità, emergono anche nodi che il negoziato dovrà necessariamente affrontare. La suddivisione del budget non è ancora dettagliata, rendendo difficile valutare l'equilibrio delle diverse componenti. La promozione della ricerca inter e transdisciplinare non appare pienamente garantita dal nuovo assetto, soprattutto alla luce della struttura a finestre tematiche dell'ECF, che rischia di ricreare silos invece di superarli.
Altri aspetti richiedono chiarimenti significativi: il futuro dei partenariati, il coordinamento tra EIC ed ECF, la definizione del perimetro del dual use, il ruolo delle PMI nei nuovi schemi progettuali, l'associazione dei Paesi terzi, la riforma del sistema di valutazione. Tutti elementi che influenzeranno in maniera determinante l'operatività di FP10.
A livello politico, il confronto tra istituzioni europee si annuncia intenso. Da una parte, la Commissione propone un quadro strategico in cui ricerca e competitività si integrano in una logica di risposta a sfide economiche e geopolitiche urgenti. Dall'altra, Parlamento e Consiglio difendono l'autonomia del Programma quadro e chiedono un bilanciamento più chiaro tra ricerca orientata all'impatto e ricerca orientata alla conoscenza. La discussione non riguarda più, come accadeva all'inizio del ciclo, la struttura generale di Horizon o la continuità con gli strumenti esistenti: riguarda piuttosto il **ruolo sistemico della R&I** nell'Europa dei prossimi decenni.
In questo quadro complesso, la comunità della ricerca europea ha mostrato una notevole compattezza. La richiesta è chiara: un Programma quadro ambizioso, autonomo, riconoscibile, dotato di governance dedicata e di capacità di integrare le diverse componenti di un sistema di R&I vivo, multidisciplinare e connesso con la società. Un Programma che non si limiti a sostenere l'innovazione industriale, ma che continui a rappresentare la piattaforma attraverso cui l'Europa costruisce conoscenza, forma talenti, coopera a livello internazionale e orienta le grandi transizioni in corso.
La fase negoziale che si apre ora sarà determinante. Il rischio, chiaramente percepito, è che la pressione delle urgenze geopolitiche e industriali finisca per comprimere spazi e ambizioni della ricerca a favore di logiche più immediate. La sfida è invece mantenere un equilibrio che consenta di **rafforzare la competitività europea senza rinunciare alla visione di lungo periodo** che ha reso i Programmi quadro uno dei pilastri più solidi dell'integrazione europea.
Per questo serve oggi una comunità della ricerca vigile e consapevole, capace di contribuire al dibattito non solo per difendere strumenti o risorse, ma per affermare un'idea di Europa fondata sulla conoscenza, sulla cooperazione e sull'ambizione strategica. Il negoziato su FP10 non riguarda soltanto un programma di finanziamento: riguarda il modello di sviluppo che l'Europa intende perseguire in un decennio decisivo. E, come sempre, la qualità delle scelte che sapremo compiere dipenderà dalla qualità del confronto che saremo in grado di mantenere.

• apre.it

La complementarità con l'European Competitiveness Fund è necessaria, ma deve salvaguardare un principio fondamentale: nell'economia della conoscenza, è la ricerca a trainare l'industria, non viceversa

Il pilastro invisibile dell'autonomia digitale in Europa

Un incontro di alto livello a Bruxelles per il futuro digitale del continente all'insegna della ricerca

di Elis Bertazzon

Invisibili ma necessarie, GÉANT e le reti nazionali della ricerca sono infrastrutture imprescindibili per la strategia digitale dell'Unione europea. Questo è il messaggio emerso dalla conferenza organizzata da GÉANT a Bruxelles lo scorso ottobre, che ha riunito circa 65 rappresentanti di alto livello provenienti da reti nazionali della ricerca (NREN) del continente, da sei diverse Direzioni Generali della Commissione europea, dagli Stati membri e dalle comunità universitarie e bibliotecarie. L'incontro è stata l'occasione per riflettere sui risultati raggiunti dalla comunità GÉANT negli ultimi anni e sulle prospettive future in un contesto segnato da rapidi cambiamenti tecnologici e geopolitici, anche in vista dell'avvio di un nuovo ciclo di finanziamento pluriennale dell'Unione, il MFF 2028.

Al centro del dibattito: connettività sicura, accesso ai dati e trasformazione digitale, elementi chiave per un'Europa digitale sovrana, competitiva e aperta alla cooperazione globale.

Un'infrastruttura digitale capillare e strategica che si estende in tutto il continente

Le reti della ricerca e i loro servizi sono un bene pubblico strategico per l'Europa, anche se, per loro natura, questi sono poco percepiti dagli utenti finali, queste le parole della CEO di GÉANT **Lise Fuhr**. Connettività ad alte prestazioni, sicurezza, gestione delle identità digitali e accesso affidabile ai dati sono oggi elementi essenziali per sostenere la cooperazione scientifica e la competitività del sistema europeo della ricerca. Appare quindi evidente come la collaborazione tra GÉANT, le NREN e la Commissione europea sia il pilastro dell'autonomia digitale per la ricerca e l'alta formazione in Europa.

Al centro del dibattito: connettività sicura, accesso ai dati e trasformazione digitale, elementi chiave per un'Europa digitale sovrana, competitiva e aperta alla cooperazione globale

Per dare un esempio di quanto sia tangibile l'impatto di queste infrastrutture digitali, spesso sottovalutate, Fuhr ha ricordato **eduroam**, uno dei servizi più riconoscibili della comunità GÉANT, che nel solo 2024 ha registrato oltre 8,4 miliardi di autenticazioni di studenti e ricercatori in tutto il mondo.

Le reti nazionali della ricerca, insieme alla dorsale europea

Le reti della ricerca rendono possibile la cosiddetta quinta libertà europea, ossia la libera circolazione della conoscenza

GÉANT, costituiscono infatti un'infrastruttura fisica capillare al servizio di circa 50 milioni di utenti in 38 paesi. Si tratta di una federazione basata su fiducia e collaborazione, capace di trasformare investimenti e competenze nazionali in un ecosistema europeo resiliente, interoperabile e sostenibile. Per questo motivo sono necessarie politiche europee coerenti e investimenti di lungo periodo nelle infrastrutture digitali pubbliche, per rafforzare l'autonomia digitale dell'Europa e ridurre la frammentazione degli interventi.
In questo contesto, si inserisce anche la **Strategia GÉANT 2026**, che mira a rafforzare il posizionamento di GÉANT insieme alle NREN nazionali come infrastruttura digitale di riferimento per la ricerca europea, aumentando la visibilità e il dialogo con le istituzioni europee a Bruxelles. L'obiettivo è rendere più evidente, anche a livello politico, il valore generato da GÉANT e dalle NREN, contribuendo in modo proattivo alla definizione delle politiche europee su ricerca, innovazione e infrastrutture digitali.

Le sfide della connettività e della libertà accademica
Le reti della ricerca rendono possibile la cosiddetta "quinta libertà" europea, ossia la **libera circolazione della conoscenza**, elemento essenziale per l'economia e il progresso della scienza in Europa. Come ricordato da Liina Munari (DG CONNECT), l'Unione sta investendo in supercalcolo, AI e piattaforme digitali per la ricerca e per fare questo spetta a GÉANT connettere e rendere interoperabili questi ecosistemi. Andrea Leone (DG INTPA) ha ampliato la dimensione internazionale, richiamando l'importanza di reti affidabili e sicure per la cooperazione con regioni come i Balcani occidentali e l'Africa e per la riduzione delle dipendenze tecnologiche in un contesto geopolitico complesso. Willi Stieger (DG ENEST) ha citato iniziative, come il **progetto Medusa**, che mira a migliorare le connessioni digitali con l'Africa del Nord con lo scopo di rafforzare la connettività, contrastare la vulnerabilità delle infrastrutture esistenti (viste le crisi nel Mar Rosso) e sostenere la **strategia Global Gateway dell'UE**. Come ricordato poi da Ronan Byrne, CEO della NREN irlandese HEAnet, le reti nazionali della ricerca costituiscono un sistema vasto e capillare su tutto il continente, un insieme di asset sensibili e altamente resilienti che non solo garantiscono sicurezza e continuità dei servizi, ma rappresentano anche ambienti privilegiati per la **sperimentazione di tecnologie innovative**, consentendo di testare nuove soluzioni – dal fibre sensing ad altre applicazioni emergenti – prima che queste arrivino sul mercato. Un valore aggiunto strategico che rafforza il ruolo delle NREN e di GÉANT come infrastrutture chiave per l'innovazione europea.

Accesso ai dati: fiducia e sovranità
Affrontare il tema della liberà accademica significa soffermarsi sul delicato equilibrio tra apertura dei dati, sicurezza e sovranità digitale. Su questo, Javier López Albacete (DG RTD), Stefan Hanslik (e-IRG), Heidi Fraser-Krauss (Jisc) e Klaas Wierenga (GÉANT) hanno ribadito che la ricerca deve rimanere aperta, collaborativa e riproducibile, ma che **l'accesso ai dati richiede modelli di governance solidi e affidabili**, soprattutto quando strumenti chiave e grandi dataset risiedono al di fuori dell'Unione europea. Le federazioni EOSC sviluppate dalle NREN sono state indicate come un esempio di risposta europea a queste sfide, insieme alla necessità di ridurre la complessità per gli utenti finali e valorizzare meglio le infrastrutture esistenti.

Digital Transformation: connettività, AI e sostenibilità
La capacità delle infrastrutture pubbliche europee di tenere il passo con l'evoluzione tecnologica sarà una variabile decisiva nelle scelte del prossimo Quadro finanziario pluriennale e di FP10.
Jean-David Malo (DG RTD) ha illustrato la strategia europea per un **ecosistema digitale sovrano e competitivo**, richiamando il ruolo di iniziative come AI for Science (RAISE). Peter Szegedi (DG CNECT) ha sottolineato come l'intelligenza artificiale rappresenti ormai una vera infrastruttura trasformativa che senza la dorsale di GÉANT non potrebbe funzionare. Katrin Amunts (EBRAINS) ha evidenziato la crescente dipendenza delle scienze ad alta intensità di dati da infrastrutture integrate, mentre Kimmo Koski (CSC – IT Center for Science) ha ricordato come gli investimenti in infrastrutture digitali pubbliche producano ritorni molto elevati e siano cruciali per la competitività europea, anche alla luce delle sfide di sostenibilità dei data centre.

Una visione condivisa per il futuro
In conclusione di questo evento è emersa con chiarezza la necessità di una **collaborazione continua e strutturata** tra NREN, GÉANT e Commissione europea, come condizione essenziale per affrontare le sfide future della ricerca e dell'istruzione. L'Europa ha bisogno di infrastrutture digitali allineate, interoperabili e federate, capaci di garantire un accesso semplice e sicuro a dati e risorse digitali. Con questa iniziativa, GÉANT insieme a tutte le NREN hanno confermato il proprio ruolo di attori chiave della trasformazione digitale europea, unendo infrastrutture, competenze e comunità per rafforzare l'economia della conoscenza e la competitività dell'Unione nel lungo periodo.

• dte.geant.org

Sono necessarie politiche europee coerenti e investimenti di lungo periodo nelle infrastrutture digitali pubbliche, per rafforzare l'autonomia digitale dell'Europa e ridurre la frammentazione degli interventi

Internet è di tutti. 25 anni di ISOC a difesa di un bene comune

di Stefano Giordano
Presidente del Chapter Italiano di Internet Society

Quando, nel 1992, un piccolo gruppo di pionieri dell'allora nascente comunità Internet si riunì a Kobe, in Giappone, per fondare la Internet Society (ISOC), il mondo della rete era ancora un territorio da esplorare. Tra quei protagonisti c'erano anche alcuni di coloro che, nel 2001, avrebbero dato vita al Chapter Italiano, contribuendo a costruire un ponte tra la visione globale di Internet e le specificità del nostro Paese.

A distanza di venticinque anni dalla nascita del capitolo italiano, ISOC continua a rappresentare un punto di riferimento per chiunque creda in un'idea di **Internet come bene comune**: aperto, globale, sicuro e realmente accessibile a tutte e tutti.

La frase che meglio riassume la filosofia dell'Internet Society è un'affermazione tanto semplice quanto rivoluzionaria: "The Internet is for Everyone." A formularla, nel 1999, fu Vinton G. Cerf, uno dei padri fondatori della rete e co-fondatore di ISOC, che nel famoso testo "The Internet is for Everyone (But it Won't Be if ...) avvertiva come la rete rischiasse di diventare terreno fertile per **nuove disuguaglianze**, monopoli, censure e concentrazioni di potere se non fosse stata difesa e progettata con responsabilità.

Quell'avvertimento è diventato la vision ufficiale dell'Internet Society e ancora oggi rappresenta la stella polare dell'intera comunità. La missione di ISOC è chiara: sostenere e promuovere lo sviluppo di Internet come infrastruttura globale, come risorsa che arricchisce la vita delle persone e come forza positiva per la società.

La missione di ISOC è chiara: sostenere e promuovere lo sviluppo di Internet come infrastruttura globale, come forza positiva per la società

Nel nostro Paese, ciò significa lavorare ogni giorno su temi che sono diventati pilastri della cultura digitale:

Accessibilità universale: nessuno deve essere escluso dalla rete per motivi economici, geografici, politici, fisici o culturali;

Libertà e apertura: Internet deve rimanere una piattaforma interoperabile, priva di barriere artificiali e accessibile all'innovazione bottom-up;

Inclusione digitale: non solo utenti: cittadini digitali attivi, capaci di partecipare, creare, contribuire,

Diritti e libertà fondamentali: privacy, libertà di espressione, diritto alla conoscenza sono elementi essenziali della società dell'informazione e della conoscenza;

Sviluppo sostenibile: la trasformazione digitale non può essere disgiunta dalla sostenibilità economica, ambientale

Il futuro della rete richiederà tecnologie aperte, a cui si possa "mettere le mani dentro", competenze diffuse, la consapevolezza che innovazione significa anche assumersi responsabilità e una forte attenzione human-centric

e sociale. Internet non è solo un'infrastruttura, ma anche uno strumento per migliorare l'educazione, l'economia e la coesione sociale;

Governance partecipativa: le regole della rete non appartengono solo ai governi ma devono essere costruite insieme a tecnici, aziende, istituzioni, accademia, comunità civiche, volontari.

Il Chapter Italiano incarna questa filosofia attraverso una comunità eterogenea: ingegneri, giuristi, sociologi, imprenditori, psicologi, studenti, pionieri della rete e semplici appassionati. È proprio nella diversità di questi contributi che risiede la forza dell'associazione: nessuno, da solo, potrebbe avere lo stesso impatto.

Nel tempo, Internet si è trasformata: non è più solo un "postino di bit" ma è diventata una piattaforma integrata che unisce comunicazione, processamento, storage e sensing, abilitando soluzioni complesse e spesso altamente specialistiche.

Il futuro della rete, in Italia come nel mondo, richiederà tecnologie aperte, a cui si possa "mettere le mani dentro", competenze diffuse, la consapevolezza che innovazione significa anche assumersi responsabilità, una forte attenzione human-centric.

Le maggiori innovazioni della storia di Internet sono nate proprio dove gli utenti hanno potuto sperimentare, rischiare, costruire. Ma la tecnologia non può sostituire la responsabilità umana: per questo **ISOC continuerà a promuovere una cultura che mette al centro le persone, i territori, le comunità, le imprese, non solo i grandi player globali**.

Oggi la sfida è fare in modo che la rete continui ad essere un bene comune, uno strumento per migliorare la salute, il lavoro, l'educazione, lo sviluppo umano e la coesione sociale.

Celebrare il venticinquennale del capitolo italiano significa quindi riconoscere il valore di una comunità che da anni lavora con rispetto, apertura e responsabilità.

Significa ribadire che Internet è un patrimonio di tutti, e che il suo futuro dipende da noi: da come scegliamo di governarlo, svilupparlo, proteggerlo.

Internet è per tutti. Ma soprattutto, Internet è di tutti.

• isoc.it

📷 Alcuni scatti della giornata celebrativa dei 25 anni di ISOC che si è svolta il 28 novembre a Novara. Foto di Sergio Bertani

Le sedi connesse alla rete GARR

La rete GARR è realizzata e gestita dal Consortium GARR, un'associazione senza fini di lucro fondata sotto l'egida del Ministero dell'Università e della Ricerca. La rete GARR è diffusa in modo capillare e offre connettività a circa 1000 sedi.

Enti soci

Consiglio Nazionale delle Ricerche · ENEA · Fondazione CRUI · INAF · INFN Istituto Nazionale di Fisica Nucleare · INGV · IRCCS IZS

CNR

- Area della Ricerca di Bari
- Area della Ricerca di Bologna
- Area della Ricerca di Catania
- Area della Ricerca di Cosenza
- Area della Ricerca di Firenze
- Area della Ricerca di Genova
- Area della Ricerca di Lecce
- Area della Ricerca di Milano 1
- Area della Ricerca di Milano 3
- Area della Ricerca di Milano 4
- Area della Ricerca di Napoli
- Area della Ricerca di Padova
- Area della Ricerca di Palermo
- Area della Ricerca di Pisa
- Area della Ricerca di Portici (NA)
- Area della Ricerca di Potenza
- Area della Ricerca di Pozzuoli (NA)
- Area della Ricerca di Roma 1
- Area della Ricerca di Roma 2
- Area della Ricerca di Sassari
- Area della Ricerca di Torino
- Base radar, Torchiarolo (BR)
- Biblioteca Area della Ricerca, Bologna
- Biomics Bioinformatica per le Scienze Omiche, Bari
- Complesso di Anacapri, ex Osservatorio Solare Svedese, Anacapri (NA)
- IAC Ist. per le Applicazioni del Calcolo M. Picone, Napoli
- IAS - Ist. per lo studio degli impatti Antropici e Sostenibilità in ambiente marino, Capo Granitola (TP), Castellammare del Golfo (TP), Oristano, Genova
- IBB Ist. di Biostrutture e Bioimmagini, Napoli
- IBBA Ist. di Biologia e Biotecnologia Agraria, Milano, Pisa
- IBBE Ist. di Biomembrane e Bioenergetica, Bari
- IBBR Ist. Bioscienze e BioRisorse, Palermo, Portici (NA)
- IBCN Ist. di Biologia Cellulare e Neurobiologia, Monterotondo Scalo (RM)
- IBE Ist. per la BioEconomia, Bologna, Firenze, Follonica (GR), San Michele Adige (TN), Sassari, Livorno, Sesto Fiorentino (FI)
- IBF Ist. di Biofisica, Genova, Pisa
- IBFM Ist. di Bioimmagini e Fisiologia Molecolare, Milano
- IBP Ist. di Biochimica delle Proteine, Napoli
- ICAR Ist. di Calcolo e Reti ad Alte Prestazioni-Palermo, Napoli, Arcavacata di Rende (CS)
- ICB Ist. di Chimica Biomolecolare, Catania, Pozzuoli (NA), Sassari
- ICCOM Ist. di Chimica dei Composti Organo Metallici, Bari, Pisa
- ICMATE Ist. di Chimica della Materia Condensata e di Tecnologie per l'Energia, Lecco
- ICVBC Ist. per la Conservazione e la Valorizzazione dei Beni Culturali, Milano
- IEIIT Ist. di Elettronica e Ingegneria dell'Informazione e delle Telecomunicazioni, Genova
- IENI Ist. per l'Energetica e le Interfasi, Genova, Milano, Padova
- IEOS Ist. per l'Endocrinologia e l'Oncologia "Gaetano Salvatore", Napoli
- IFC Ist. di Fisiologia Clinica, Lecce, Massa Carrara, Milano, Pisa, Reggio Calabria
- IFT Ist. Farmacologia Traslazionale, L'Aquila
- IGAG Ist. di Geologia Ambientale e Geoingegneria, Milano
- IGB Ist. di Genetica e Biofisica "Adriano Buzzati Traverso", Napoli
- IGG Ist. di Geoscienze e Georisorse, Pavia, Pisa, Torino
- IGM Ist. di Genetica Molecolare, Chieti, Pavia
- IIT Ist. di Informatica e Telematica, Pisa, Arcavacata di Rende (CS)
- ILC Ist. di Linguistica Computazionale, Pisa, Genova
- IMAA Ist. di Metodologie per l'Analisi Ambientale, Tito Scalo (PZ), Marsico Nuovo (PZ)
- IMATI Ist. di Matematica Applicata e Tecnologie Informatiche "E. Magenes", Genova, Milano, Pavia
- IMEM Ist. dei Materiali per l' Elettronica ed il Magnetismo, Parma
- IMM Ist. per la Microelettronica e i Microsistemi, Agrate Brianza (MB), Bologna, Catania, Lecce, Roma
- IN Ist. di Neuroscienze, Milano, Pisa
- INM Ist. di Ingegneria del Mare (INM), Roma
- INO Ist. Nazionale di Ottica, Firenze, Pisa, Pozzuoli (NA)
- IOM Ist. Officina dei Materiali, Trieste
- IPCB Ist. per i Polimeri, Compositi e Biomateriali, Catania, Napoli, Portici (NA), Pozzuoli (NA)
- IPCF Ist. di Tecnologie Biomediche, Bari, Pisa, Messina
- IPSP Ist. per la Protezione Sostenibile delle Piante, Bari, Portici (NA), Torino
- IRBIM Ist. per le Risorse Biologiche e le Biotecnologie Marine, Ancona, Mazara del Vallo (TP), Messina
- IRCrES Ist. di Ricerca sulla Crescita Economica Sostenibile, Milano, Moncalieri (TO), Torino
- IREA Ist. per il Rilevamento Elettromagnetico dell'Ambiente, Milano, Napoli
- IRET Ist. di Ricerca sugli Ecosistemi Terrestri, Napoli, Porano (TR), Sassari
- IRGB Ist. di Ricerca Genetica e Biomedica, Lanusei (OG), Monserrato (CA), Sassari
- IRIB Ist. per la Ricerca e l'Innovazione Biomedica, Catanzaro, Messina
- IRISS Ist. di Ricerca su Innovazione e Servizi per lo Sviluppo, Napoli
- IRPI Ist. di Ricerca per la Protezione Idrogeologica, Padova, Perugia, Torino
- IRPPS Ist. di Ricerche sulla Popolazione e le Politiche Sociali, Penta di Fisciano (SA), Roma
- IRSA Ist. di Ricerca sulle Acque, Bari, Brugherio (MB), Taranto, Verbania Pallanza (VB)
- ISA Ist. di Scienze dell'Alimentazione, Avellino
- ISAC Ist. di Scienze dell'Atmosfera e del Clima, Bologna, Lamezia Terme (CZ), Lecce, Padova, Torino
- ISAFoM Ist. per i Sistemi Agricoli e Forestali del Mediterraneo, Ercolano (NA)
- ISASI Ist. di Scienze Applicate e Sistemi Intelligenti "Eduardo Caianiello", Napoli, Pozzuoli (NA)
- ISE Ist. per lo Studio degli Ecosistemi, Pisa
- ISEM Ist. di Storia dell'Europa Mediterranea, Cagliari, Roma
- ISIB Ist. di Ingegneria Biomedica, Padova
- ISM Ist. di Struttura della Materia, Tito Scalo (PZ), Trieste
- ISMAC Ist. per lo Studio delle Macromolecole, Milano
- ISMAR Ist. di Scienze Marine, Bologna, Genova, Lesina (FG), Napoli, Pozzuolo di Lerici (SP), Trieste, Venezia
- ISMed Ist. di Studi sul Mediterraneo, Napoli
- ISMN Ist. per lo Studio dei Materiali

Nanostrutturati, Bologna
- ISN Ist. di Scienze Neurologiche, Catania, Mangone (CS)
- ISOF Ist. per la Sintesi Organica e la Fotoreattività, Bologna
- ISP Ist. di Scienze Polari, Padova
- ISPA Ist. di Scienze delle Produzioni Alimentari, Foggia, Lecce, Oristano, Sassari
- ISPAAM Ist. per il Sistema Produzione Animale in Ambiente Mediterraneo, Napoli, Sassari
- ISPC Ist. di Scienze del Patrimonio Culturale, Lecce, Tito Scalo (PZ)
- ISPF Ist. per la Storia del Pensiero Filosofico e Scientifico Moderno, Milano
- ISSIA Ist. di Studi sui Sistemi Intelligenti per l'Automazione, Genova
- ISSMC, Ist. di Scienza, Tecnologia e Sostenibilità per lo Sviluppo dei Materiali Ceramici, Faenza (RA)
- ISTC Ist. di Scienze e Tecnologie della Cognizione, Padova, Roma
- ISTEC Ist. di Scienza e Tecnologia dei Materiali Ceramici, Torino
- ISTI Ist. di Scienza e Tecnologie dell'Informazione, Pisa
- ISTM Ist. di Scienze e Tecnologie Molecolari, Milano
- ISTP Ist. per la Scienza e Tecnologia dei Plasmi, Milano, Padova
- ITAE Ist. di Tecnologie Avanzate per l'Energia, Messina
- ITB Ist. di Tecnologie Biomediche, Pisa, Segrate (MI)
- ITC Ist. per le tecnologie della costruzione, Bari, L'Aquila, Milano, Padova, San Giuliano Milanese (MI)
- ITD Ist. per le Tecnologie Didattiche, Genova
- ITM Ist. per la Tecnologia delle Membrane, Arcavacata di Rende (CS)
- ITTIG Ist. di Teoria e Tecniche dell'Informazione Giuridica, Firenze
- NANOTEC Ist. di Nanotecnologia, Lecce, Bari
- OVI Ist. del Vocabolario Italiano, Firenze
- SCITEC Ist. di Scienze e Tecnologie Chimiche "Giulio Natta", Genova, Milano, Roma
- Sede Centrale, Roma
- SPIN Ist. per i Superconduttori, Materiali Innovativi e Dispositivi, Genova
- SPR RSI Struttura di Particolare Rilievo Reti e Sistemi Informativi, Roges di Rende (CS)
- STEMS - Ist. di Scienze e Tecnologie per l'Energia e la Mobilità Sostenibili, Candiolo (TO), Cassana (FE), Napoli, Torino
- STIIMA Ist. di Sistemi e Tecnologie Industriali Intelligenti per il Manifatturiero Avanzato, Biella, Milano
- UARIE - Ufficio Attività e Relazioni con Istituzioni Europee, Napoli

ENEA

- Centro ricerche Ambiente Marino S. Teresa, Pozzuolo di Lerici (SP)
- Centro ricerche Bologna
- Centro ricerche Brasimone, Camugnano (BO)
- Centro ricerche Brindisi
- Centro ricerche Casaccia, S.Maria di Galeria (RM)
- Centro ricerche Frascati (RM)
- Centro ricerche Portici (NA)
- Centro ricerche Saluggia (VC)
- Centro ricerche Trisaia, Rotondella (MT)
- Laboratori di ricerca Faenza (RA)
- Laboratori di ricerca Foggia
- Laboratori di ricerca Ispra (VA)
- Laboratori di ricerca Lampedusa (AG)
- Laboratori di ricerca Montecuccolino, Bologna
- Sede centrale, Roma
- Ufficio territoriale della Puglia, Bari
- Ufficio territoriale della Sicilia, Palermo
- Ufficio territoriale della Toscana, Pisa

INAF

- CTA Cherenkov Telescope Array, Roma
- IASF Istituto di Astrofisica Spaziale e Fisica Cosmica, Bologna, Milano, Palermo
- OAC SRT Sardinia Radio Telescope, S. Basilio (CA)
- IRA Istituto di Radioastronomia, Bologna, Staz. Radioastronomica di Noto (SR), Staz. Radioastronomica di Medicina (BO)
- Laboratorio di Astrofisica di Palermo
- Osservatorio Astrofisico di Arcetri (FI)
- Osservatorio Astrofisico di Catania
- Osservatorio Astronomico di Abruzzo, Teramo
- Osservatorio Astronomico di Bologna
- Osservatorio Astronomico di Brera, Merate (LC), Milano
- Osservatorio Astronomico di Cagliari, Selargius (CA)
- Osservatorio Astronomico di Capodimonte, Napoli
- Osservatorio Astronomico di Padova
- Osservatorio Astronomico di Palermo
- Osservatorio Astronomico di Roma, Monte Porzio Catone (RM)
- Osservatorio Astronomico di Torino, Pino Torinese (TO)
- Osservatorio Astronomico di Trieste
- Presidenza, Roma

INFN

- Amministrazione centrale, Frascati (RM)
- CNAF Centro Nazionale per la ricerca e lo sviluppo nelle tecnologie informatiche e telematiche, Bologna
- Gruppo collegato dell'Aquila
- Gruppo collegato di Alessandria
- Gruppo collegato di Brescia
- Gruppo collegato di Cosenza
- Gruppo collegato di Messina
- Gruppo collegato di Parma
- Gruppo collegato di Salerno
- Gruppo collegato di Siena
- Gruppo collegato di Udine
- Laboratori Nazionali del Gran Sasso, Assergi (AQ)
- Laboratori Nazionali del Sud, Catania
- Laboratori Nazionali di Frascati (RM)
- Laboratori Nazionali di Legnaro (PD)
- Laboratorio Portopalo di Capo Passero (SR)
- Sezione di Bari
- Sezione di Bologna
- Sezione di Cagliari
- Sezione di Catania
- Sezione di Ferrara
- Sezione di Firenze
- Sezione di Genova
- Sezione di Lecce
- Sezione di Milano
- Sezione di Milano-Bicocca
- Sezione di Napoli
- Sezione di Padova
- Sezione di Pavia
- Sezione di Perugia
- Sezione di Pisa
- Sezione di Roma
- Sezione di Roma-Tor Vergata
- Sezione di Roma Tre
- Sezione di Torino
- Sezione di Trieste
- TIFPA Trento Institute for Fundamental Phisycs and Application, Povo (TN)
- Uffici di Presidenza, Roma

INGV

- Amministrazione Centrale, Roma
- Sede distaccata di Grottaminarda (AV), Irpinia
- Sede distaccata di Lipari (ME), Osservatorio Geofisico
- Sede distaccata di Nicolosi (CT)
- Sede distaccata di Stromboli (ME), Centro Operativo
- Sezione di Bologna
- Sezione di Catania, CUAD Sistema Poseidon
- Sezione di Catania, Osservatorio Etneo
- Sezione di Catania, Sede di Messina
- Sezione di Cosenza
- Sede Storica, Ercolano (NA)
- Sezione di Napoli, Osservatorio Vesuviano
- Sezione di Milano
- Sezione di Messina
- Sezione di Palermo
- Sezione di Pisa
- Sezione di Portopalo di Capo Passero (SR)

IRCCS Istituti di Ricovero e Cura a Carattere Scientifico

- Azienda Ospedaliero Universitaria, Bologna
- Azienda Ospedaliera Universitaria Meyer, Firenze

- Centro Cardiologico S.P.A. Fondazione Monzino, Milano
- Centro Neurolesi Bonino Pulejo, Messina
- Centro San Giovanni di Dio Fatebenefratelli, Brescia
- CROB Centro di riferimento oncologico della Basilicata, Rionero in Vulture (PZ)
- CRO Centro di Riferimento Oncologico, Aviano (PN)
- Ente Ospedaliero specializzato in gastroenterologia Saverio De Bellis, Castellana Grotte (BA)
- Fondazione Ca'Granda – Ospedale Maggiore Policlinico, Milano
- Fondazione del Piemonte per l'Oncologia, Candiolo (TO)
- Fondazione Don Carlo Gnocchi, Milano
- Fondazione G.B. Bietti per lo studio e la ricerca in oftalmologia, Roma
- Fondazione IRCCS Ist. Nazionale dei tumori, Milano
- Fondazione Ist. Neurologico Carlo Besta, Milano
- Fondazione Ist. Neurologico Casimiro Mondino, Pavia
- Fondazione Policlinico San Matteo, Pavia
- Fondazione Policlinico Universitario Gemelli, Roma
- Fondazione San Gerardo dei Tintori, Monza
- Fondazione Santa Lucia, Roma
- Fondazione Stella Maris, Calambrone (PI)
- IDI Ist. Dermopatico dell'Immacolata, Roma
- IEO Ist. Europeo di Oncologia, Milano
- IFO Ist. Fisioterapici Ospitalieri, Ist. Dermatologico Santa Maria e San Gallicano, Roma
- ISMETT Ist. Mediterraneo per i Trapianti e Terapie ad Alta Specializzazione, Palermo
- Ist. Auxologico Italiano, Milano
- Ist. Clinici Scientifici Maugeri, Pavia
- Ist. Clinico Humanitas, Rozzano (Milano)
- Ist. delle Scienze Neurologiche, Bologna
- Ist. Eugenio Medea, Bosisio Parini (LC)
- Ist. Giannina Gaslini, Genova
- Ist. Mario Negri, Milano
- Ist. Nazionale di Riposo e Cura per Anziani, Ancona
- Ist. Nazionale Tumori Fondazione Giovanni Pascale, Napoli
- Ist. Neurologico Mediterraneo Neuromed, Pozzilli (IS)
- Ist. Oncologico Veneto, Padova
- Ist. Ortopedico Galeazzi, Milano
- Ist. Ortopedico Rizzoli, Bologna
- Ist. per le Malattie Infettive L. Spallanzani, Roma
- Ist. scientifico romagnolo per lo studio e la cura dei tumori, Meldola (FC)
- Ist. Tumori Giovanni Paolo II, Bari
- Multimedica, Milano
- Oasi di Maria Santissima, Troina (EN)
- Ospedale Casa Sollievo della Sofferenza, San Giovanni Rotondo (FG)
- Ospedale infantile Burlo Garofolo, Trieste
- Ospedale pediatrico Bambino Gesù, Roma
- Ospedale Policlinico San Martino, Genova
- Ospedale San Raffaele, Milano
- Policlinico San Donato, S. Donato Milanese
- San Camillo IRCCS S.r.l., Venezia
- San Raffaele Pisana, Roma
- SYNLAB SDN, Napoli

IZS Istituti Zooprofilattici Sperimentali

- IZS del Lazio e della Toscana, Roma
- IZS del Mezzogiorno, Portici (NA)
- IZS del Piemonte, Liguria e Valle d'Aosta, Torino
- IZS dell'Abruzzo e del Molise G. Caporale, Teramo
- IZS dell'Umbria e delle Marche, Perugia
- IZS della Lombardia e dell'Emilia Romagna, Brescia
- IZS della Puglia e della Basilicata, Foggia
- IZS della Sardegna, Sassari
- IZS della Sicilia M. Mirri, Palermo
- IZS delle Venezie, Legnaro (PD)

Università

Università statali

- CRUI Conferenza dei Rettori delle Università Italiane, Roma
- GSSI Gran Sasso Science Institute, L'Aquila
- IMT Institutions, Markets, Technologies Institute for Advanced Studies, Lucca
- IUSS Istituto Universitario di Studi Superiori, Pavia
- Politecnico di Bari
- Politecnico di Milano
- Politecnico di Torino
- Scuola Normale Superiore, Pisa
- Scuola Superiore S.Anna, Pisa
- Scuola Superiore Meridionale
- Seconda Università degli Studi di Napoli
- SISSA Scuola Internazionale Superiore di Studi Avanzati, Trieste
- Università Ca' Foscari Venezia
- Università della Basilicata
- Università della Calabria
- Università della Tuscia
- Università dell'Aquila
- Università dell'Insubria
- Università del Molise
- Università del Piemonte Orientale Amedeo Avogadro
- Università del Salento
- Università del Sannio
- Università di Bari Aldo Moro
- Università di Bergamo
- Università di Bologna
- Università di Brescia
- Università di Cagliari
- Università di Camerino
- Università di Cassino e del Lazio Meridionale
- Università di Catania
- Università di Chieti-Pescara G. D'Annunzio
- Università di Ferrara
- Università di Firenze
- Università di Foggia
- Università di Genova
- Università di Macerata
- Università di Messina
- Università di Milano
- Università di Milano-Bicocca
- Università di Modena e Reggio Emilia
- Università di Napoli Federico II
- Università di Napoli L'Orientale
- Università di Napoli Parthenope
- Università di Padova
- Università di Palermo
- Università di Parma
- Università di Pavia
- Università di Perugia
- Università di Pisa
- Università di Roma Foro Italico
- Università di Roma La Sapienza
- Università di Roma Tor Vergata
- Università di Roma Tre
- Università di Salerno
- Università di Sassari
- Università di Siena
- Università di Teramo
- Università di Torino
- Università di Trento
- Università di Trieste
- Università di Udine
- Università di Urbino Carlo Bo
- Università di Verona
- Università IUAV di Venezia
- Università Magna Græcia di Catanzaro
- Università Mediterranea di Reggio Calabria
- Università per Stranieri di Perugia
- Università per Stranieri di Siena
- Università Politecnica delle Marche

Università non statali

- Humanitas University, Pieve Emanuele (MI)
- IULM Libera Università di Lingue e Comunicazione, Milano
- Libera Università di Bolzano
- Libera Università di Enna Kore
- LUISS Libera Università Internazionale degli Studi Sociali Guido Carli, Roma
- LUM Libera Università Mediterranea J. Monnet, Casamassima (BA)
- LUMSA Libera Università Maria SS. Assunta, Roma, Palermo
- SDA Bocconi School of Management, Roma
- UNINT Università degli Studi Internazionali di Roma

- UniTelma Sapienza, Roma
- Università Campus Bio-Medico di Roma
- Università Cattolica del Sacro Cuore, Milano
- Università Commerciale Luigi Bocconi, Milano
- Università della Valle d'Aosta, Aosta
- Università Suor Orsola Benincasa, Napoli
- Università Telematica Internazionale Uninettuno, Roma
- Università Vita-Salute San Raffaele, Milano

Università Internazionali

- Cornell University, Roma
- European University Institute, Firenze
- Johns Hopkins University, Bologna
- New York University, Firenze
- The American University of Rome, Roma
- Venice International University, Venezia

Consorzi interuniversitari, collegi, enti per il diritto allo studio

- CINECA, Napoli, Roma, Bologna
- CISIA Consorzio Interuniversitario Sistemi Integrati per l'Accesso, Pisa
- Collegio Ghislieri, Pavia
- Collegio Nuovo - Fondaz. Sandra e Enea Mattei, Pavia
- Collegio Universitario Alessandro Volta, Pavia
- Collegio Universitario Santa Caterina da Siena, Pavia

Enti di ricerca scientifica e tecnologica

- AREA Science Park, Trieste
- ARPAS Agenzia Regionale per la Protezione dell'Ambiente della Sardegna, Cagliari, Sassari
- ASI Agenzia Spaziale Italiana
  - ALTEC Advanced Logistic Technology
  - Engineering Center, Torino
  - Centro di Geodesia Spaziale, Matera
  - Centro Spaziale del Fucino, Avezzano (AQ)
  - Scientific Data Center, Roma
  - Sede Centrale, Roma
  - Sardinia Deep Space Antenna, San Basilio (CA)
- Centro Fermi - Museo Storico della Fisica e Centro Studi e Ricerche Enrico Fermi, Roma
- CERIC - ERIC Central European Research Infrastructure Consortium, Basovizza (TS)
- CIRA Centro Italiano Ricerche Aerospaziali, Capua (CE)
- CMCC Centro Euro-Mediterraneo per i Cambiamenti Climatici, Bologna, Lecce
- CNIT Laboratorio Nazionale di Comunicazioni Multimediali, Napoli
- Consorzio CETMA Centro di Progettazione, Design e Tecnologie dei Materiali, Brindisi
- Consorzio TeRN Tecnologie per le Osservazioni della Terra e i Rischi Naturali, Tito Scalo (PZ)
- CORILA Consorzio Gestione del Centro di Coordinamento delle Attività di Ricerca Inerenti al Sistema Lagunare di Venezia
- COSBI The Microsoft Research – University of Trento Centre for Computational and Systems Biology, Rovereto (TN)
- CREA Consiglio per la ricerca in agricoltura e l'analisi dell'economia agraria, Bari, Bologna, Pontecagnano (SA)
- CRS4 Centro Ricerca, Sviluppo e Studi Superiori in Sardegna, Pula (CA)
- CSP Innovazione nelle ICT, Torino
- CTAO - Cherenkov Telescope Array Observatory, Bologna
- ECMWF European Centre for Medium-Range Weather Forecasts, Bologna
- EGO European Gravitational Observatory, Cascina (PI)
- EUMETSAT European Organisation for the Exploitation of Meteorological Satellites, Avezzano (AQ)
- FBK Fondazione B. Kessler, Trento
- Fondazione E. Amaldi, Roma
- G. Galilei Institute for Theoretical Physics, Firenze
- Global Campus of Human Rights, Venezia
- Hypatia - Consorzio di Ricerca sulle Tecnologie per lo Sviluppo sostenibile, Roma
- ICRANet International Centre for Relativistic Astrophysics, Pescara
- ICTP Centro Internaz. di Fisica Teorica, Trieste
- IIT Istituto Italiano di Tecnologia, Aosta, Bari, Genova, Lecce, Milano, Napoli, Roma, Torino
- INRIM Ist. Nazionale di Ricerca Metrologica, Torino
- ISPRA Istituto Superiore per la Protezione e la Ricerca Ambientale, Livorno, Roma, Ozzano dell'Emilia (BO), Palermo, Venezia
- ISTAT Istituto Nazionale di Statistica, Roma
- LaMMA Laboratorio di Monitoraggio e Modellistica Ambientale per lo sviluppo sostenibile, Livorno, Sesto Fiorentino (FI)
- JRC Joint Research Centre, Ispra (VA)
- LENS Laboratorio Europeo di Spettroscopie Non Lineari, Firenze
- NATO CMRE, Centre for Maritime Research and Experimentation, La Spezia
- OGS Istituto Nazionale di Oceanografia e di Geofisica Sperimentale, Sgonico (TS), Udine
- Registro.it, Pisa, Milano, Roma
- Sincrotrone Trieste
- Stazione Zoologica A. Dohrn, Ischia, Messina, Napoli, Portici (NA)

Istituti di ricerca biomedica

- Azienda Ospedaliera Monaldi, Napoli
- Azienda Ospedaliero-Universitaria, Cagliari
- CBIM Consorzio di Bioingegneria e Informatica Medica, Pavia
- EMBL European Molecular Biology Laboratory, Monterotondo (RM)
- Fondazione CNAO - Centro Nazionale di Adroterapia Oncologica, Pavia
- Fondazione Human Technopole, Milano
- Fondazione Toscana Gabriele Monasterio per la Ricerca Medica e di Sanità Pubblica, Pisa
- ICGEB International Centre for Genetic Engineering and Biotechnology, Trieste
- IIGM Foundation - Italian Institute for Genomic Medicine, Torino
- ISS Istituto Superiore di Sanità, Roma
- LIGHT Center, Brescia
- TIGEM Telethon Institute of Genetics and Medicine, Napoli, Pozzuoli (NA)

Istituti di cultura, ricerca e promozione scientifica

- Accademia della Crusca, Firenze
- Accademia Nazionale dei Lincei, Roma
- Centro Congressi Ex Casinò e Palazzo del Cinema, Venezia
- Chancellerie des Universités de Paris, Villa Finaly, Firenze
- CASD - Centro Alti Studi per la Difesa Roma
- Comando per la Formazione e Scuola di Applicazione dell'Esercito di Torino
- Ecole Française de Rome
- ESCP École Supérieure de Commerce de Paris - Business School, Torino
- EURAC Accademia Europea di Bolzano
- FEEM Fondazione ENI E. Mattei, Milano, Venezia
- Fondazione Collegio Carlo Alberto - Centro di Ricerca e Alta Formazione, Torino
- Fondazione E. Majorana e Centro di Cultura Scientifica, Erice (TP)
- Fondazione Eucentre Centro Europeo di Formazione e Ricerca in Ingegneria Sismica, Pavia
- Fondazione IDIS - Città della Scienza, Napoli
- Fondazione LINKS Leading Innovation & Knowledge for Society, Torino
- Fondazione per la Scuola della Compagnia di San Paolo, Torino
- Fondazione U. Bordoni, Milano, Roma
- Fondazione Ufficio Pio della Compagnia di San Paolo, Torino
- Fondazione 1563 per l'Arte e la Cultura della Compagnia di San Paolo, Torino
- Gabinetto Scientifico Letterario G.P. Vieusseux, Firenze
- GSoM Graduate School of Management, Milano
- INSR Ist. Nazionale di Studi sul Rinascimento, Firenze
- Istituto di Norvegia in Roma
- IVSLA Istituto Veneto, Accademia di Scienze, Lettere ed Arti, Venezia
- Kunsthistorisches Institut in Florenz - M.Planck Institut, Firenze
- LIS Laboratorio dell'Immaginario Scientifico, Grignano (TS)
- MIB - School of Management, Trieste
- MUGEOS, Museo di Geoscienze, Rocca di Papa (RM)
- MUSE Museo delle Scienze, Trento
- Museo Galileo - Istituto e Museo di Storia della Scienza, Firenze
- San Servolo Servizi Metropolitani di Venezia

Archivi, biblioteche, musei

- Archivio di Stato di Bologna
- Archivio di Stato Centrale, Roma
- Archivio di Stato di Milano
- Archivio di Stato di Napoli
- Archivio di Stato di Palermo
- Archivio di Stato di Roma
- Archivio di Stato di Torino
- Archivio di Stato di Torino - Sezioni Riunite
- Archivio di Stato di Venezia
- Biblioteca Angelica, Roma
- Biblioteca Casanatense, Roma
- Biblioteca di Storia Moderna e Contemporanea, Roma
- Biblioteca Estense e Universitaria, Modena
- Biblioteca Marucelliana, Firenze
- Biblioteca Medica Statale, Roma
- Biblioteca Medicea Laurenziana, Firenze
- Biblioteca Nazionale Braidense, Milano
- Biblioteca Nazionale Centrale di Firenze
- Biblioteca Nazionale Centrale V. Emanuele II di Roma
- Biblioteca Nazionale Marciana, Venezia
- Biblioteca Nazionale Universitaria di Torino
- Biblioteca Palatina, Parma
- Biblioteca Riccardiana, Firenze
- Biblioteca Statale Antonio Baldini, Roma
- Biblioteca Statale di Trieste
- Biblioteca Universitaria Alessandrina, Roma
- Biblioteca Universitaria di Bologna
- Biblioteca Universitaria di Genova
- Biblioteca Universitaria di Napoli
- Biblioteca Universitaria di Padova
- Biblioteca Universitaria di Pavia
- Biblioteca Universitaria di Pisa
- Bibliotheca Hertziana Ist. M. Planck per la Storia dell'Arte, Roma
- Fondazione Palazzo Strozzi, Firenze
- Galleria dell'Accademia di Firenze
- Gallerie degli Uffizi, Firenze
- ICCU Ist. Centrale per il Catalogo Unico delle Biblioteche Italiane e per le Informazioni bibliografiche, Roma
- Ist. Centrale per gli Archivi, Roma
- Ist. Centrale per i Beni Sonori ed Audiovisivi. Roma
- Ministero della Cultura - Direzione Generale Educazione, ricerca e istituti culturali, Roma
- Museo Nazionale Romano - Crypta Balbi, Palazzo Altemps, Palazzo Massimo, Terme di Diocleziano
- Museo Storico e il Parco del Castello di Miramare, Trieste
- Parco Archeologico del Colosseo, Roma - Colosseo e Palatino, via in Miranda
- Parco Archeologico di Pompei
- Procuratoria di San Marco, Venezia

Accademie, conservatori, istituti d'arte

- Accademia di Belle Arti di Bologna
- Accademia di Belle Arti di Brera, Milano
- Accademia di Belle Arti di Firenze
- Accademia di Belle Arti de L'Aquila
- Accademia di Belle Arti di Macerata
- Accademia di Belle Arti di Palermo
- Accademia di Belle Arti di Perugia
- Accademia di Belle Arti di Roma
- Accademia di Belle Arti di Urbino
- Accademia di Belle Arti di Venezia
- Conservatorio di Musica D. Cimarosa, Avellino
- Conservatorio di Musica N. Piccinni, Bari
- Conservatorio di Musica C. Monteverdi, Bolzano
- Conservatorio di Musica G. Verdi, Como
- Conservatorio di Musica S. Giacomantonio, Cosenza
- Conservatorio di Musica C. Monteverdi, Cremona
- Conservatorio di Musica G.F. Ghedini, Cuneo
- Conservatorio di Musica G. Frescobaldi, Ferrara
- Conservatorio di Musica L. Cherubini, Firenze
- Conservatorio di Musica L. Refice, Frosinone
- Conservatorio di Musica N. Paganini, Genova
- Conservatorio di Musica Egidio R. Duni, Matera
- Conservatorio di Musica G. Puccini, La Spezia
- Conservatorio di Musica P. Mascagni, Livorno
- Conservatorio di Musica G. Verdi, Milano
- Conservatorio di Musica G. Cantelli, Novara
- Conservatorio di Musica C. Pollini, Padova
- Conservatorio di Musica A. Boito, Parma
- Conservatorio di Musica A. Casella, L'Aquila
- Conservatorio di Musica T. Schipa, Lecce
- Conservatorio di Musica Vecchi Tonelli, Modena
- Conservatorio di Musica A. Scarlatti, Palermo
- Conservatorio di Musica F. Vittadini, Pavia
- Conservatorio di Musica G. Lettimi, Rimini
- Conservatorio di Musica Santa Cecilia, Roma
- Conservatorio di Musica G. Martucci, Salerno
- Conservatorio di Musica R. Franci, Siena
- Conservatorio di Musica G. Tartini, Trieste
- Conservatorio di Musica J. Tomadini, Udine
- Ist. Superiore per le Industrie Artistiche, Faenza (RA)
- Ist. Superiore per le Industrie Artistiche, Urbino

Scuole

Piemonte

- Convitto Nazionale Umberto I, Torino
- Liceo Statale Regina Margherita, Collegno (TO)
- Liceo Scientifico Ferraris, Torino
- ITI Majorana, Grugliasco (TO)
- IIS M. Curie - C. Levi, Collegno (TO)
- IIS Avogadro, Torino
- IIS Santorre di Santarosa, Torino
- ITIS Pininfarina, Moncalieri (TO)

Lombardia

- ISIS Carcano, Como
- IPS Pessina, Como
- ITE Caio Plinio II, Como
- Liceo Scientifico e Classico Majorana, Desio (MB)
- Scuola Europea di Varese

Veneto

- ITC Einaudi-Gramsci, Padova
- ITIS Severi, Padova
- Liceo delle Scienze Umane Amedeo di Savoia Duca d'Aosta, Padova
- Liceo Artistico Modigliani, Padova

Friuli Venezia-Giulia

- IT Zanon, Udine
- Liceo Marinelli, Udine
- Liceo Scientifico Galilei, Trieste
- Liceo Scientifico Oberdan, Trieste

Emilia-Romagna

- Scuole connesse nell'ambito della collaborazione con la rete dell'Emilia-Romagna Lepida

Liguria

- Convitto Nazionale Colombo, Genova
- IIS Ferraris-Pancaldo, Savona
- IIS Vittorio Emanuele II - Ruffini, Genova

Toscana

- IIS Cellini, Firenze
- IIS Enriques Agnoletti, Sesto Fiorentino (FI)
- IIS Salvemini-D'Aosta, Firenze
- IIS Vespucci-Colombo, Livorno
- IPSIA Fascetti, Pisa
- IPSSAR Matteotti, Pisa
- ISIS Leonardo da Vinci, Firenze
- IT Cappellini, Livorno
- ITC Pacinotti, Pisa
- ITIS Galileo Galilei, Livorno
- ITIS Leonardo da Vinci, Pisa
- Liceo Artistico Russoli, Pisa
- Liceo Classico Galileo Galilei, Pisa
- Liceo Scientifico Buonarroti, Pisa
- Liceo Scientifico Dini, Pisa
- Liceo Statale Carducci, Pisa
- Liceo Statale Federigo Enriques, Livorno
- Polo Liceale Francesco Cecioni, Livorno

Marche

- IIS Volterra Elia, Ancona
- ITIS Mattei, Urbino
- Liceo Scientifico Galilei, Ancona
- Liceo Scientifico e delle Scienze Umane Laurana-Baldi, Urbino

Lazio

- Convitto Nazionale Vittorio Emanuele II, Roma
- IIS Einaudi-Baronio, Sora (FR)

- IIS Caffè, Roma
- IIS Medaglia D'Oro, Cassino (FR)
- Istituto Magistrale Statale Gelasio Caetani, Roma
- ITCG Ceccherelli, Roma
- ITI Ferraris, Roma
- ITIS Majorana, Cassino
- ITIS Volta, Roma
- IT Nautico Colonna, Roma
- ITS Meccatronico, Frosinone
- ITS Pascal, Roma
- ITST Istituto Tecnico Fermi, Frascati (RM)
- Liceo Scientifico Malpighi, Roma
- Liceo Scientifico Plinio Seniore, Roma
- Liceo Statale Ginnasio Virgilio, Roma

Campania

- Convitto Nazionale Vittorio Emanuele II, Napoli
- IIS Casanova, Napoli
- IIS Don Lorenzo Milani, Gragnano (NA)
- IIS Livatino, Napoli
- IIS Nitti, Napoli
- IPIA Marconi, Giugliano in Campania (NA)
- IPSSAR Rossi Doria, Avellino
- ISIS Pagano-Bernini, Napoli
- ISIS Vittorio Emanuele II, Napoli
- Ist. Polispecialistico San Paolo, Sorrento (NA)
- ITIS Focaccia, Salerno
- ITIS Giordani, Caserta
- ITIS Giordani-Striano, Napoli
- ITIS Luigi Galvani, Giugliano in Campania (NA)
- Liceo Classico Carducci, Nola (CE)
- Liceo Classico Tasso, Salerno
- Liceo Classico Vittorio Emanuele II, Napoli
- Liceo Scientifico De Carlo, Giugliano in Campania (NA)
- Liceo Scientifico Genoino, Cava dè Tirreni (SA)
- Liceo Scientifico Segrè, Marano di Napoli (NA)
- Liceo Scientifico Tito Lucrezio Caro, Napoli
- Liceo Scientifico Vittorini, Napoli

Puglia

- IC Mazzini-Modugno, Bari
- IC Perotti-Ruffo, Cassano delle Murge (BA)
- IIS Carafa, Andria
- IIS Carelli-Forlani, Conversano (BA)
- IIS Colasanto, Andria
- IIS Copertino, Copertino (LE)
- IIS Marzolla-Simone-Durano, Brindisi
- IIS Medi, Galatone (LE)
- IIS Pacinotti-Fermi, Taranto
- IIS Perrone, Castellaneta (TA)
- IIS Righi, Cerignola (FG)
- IISS Da Vinci, Fasano (BR)
- IISS De Pace, Lecce
- IISS Euclide, Bari
- IISS Majorana, Brindisi
- IISS Majorana, Martina Franca (TA)
- IISS Trinchese, Martano (LE)
- IPSSAR Pertini, Brindisi
- ISIS Fermi, Lecce
- ISIS Righi, Taranto
- ITE Carlo Levi, Andria
- ITE e LL Marco Polo, Bari
- ITE Giordano, Bitonto (BA)
- ITE Lenoci, Bari
- ITELL Giulio Cesare, Bari
- ITE Pascal, Foggia
- ITIS Fermi, Francavilla Fontana (BR)
- ITIS Giorgi, Brindisi
- ITIS Jannuzzi, Andria
- ITIS Modesto Panetti, Bari
- IT Pitagora, Bari
- ITS Elena di Savoia, Bari
- ITT Altamura-Da Vinci, Foggia
- Liceo Carolina Poerio, Foggia
- Liceo Classico e Musicale Palmieri, Lecce
- Liceo Don Milani, Acquaviva delle Fonti (BA)
- Liceo Scientifico e Linguistico Vallone, Galatina (LE)
- Liceo Scientifico Fermi-Monticelli, Brindisi
- Liceo Scientifico Galilei, Bitonto (BA)
- Liceo Scientifico Salvemini, Bari
- Liceo Scientifico Scacchi, Bari
- Liceo Tito Livio, Martina Franca (TA)
- Scuola Sec. I Grado Michelangelo, Bari
- Secondo IC, Francavilla Fontana (BR)

Calabria

- IIS Fermi, Catanzaro Lido
- IPSSEOA Soverato (CZ)
- IT Calabretta, Soverato (CZ)
- ITE De Fazio, Lamezia Terme (CZ)
- ITI Scalfaro, Catanzaro
- ITIS Monaco, Cosenza
- Liceo Scientifico Guarasci, Soverato (CZ)
- Liceo Scientifico Pitagora, Rende (CS)

Sicilia

- IC Battisti, Catania
- IIS Ferrara, Mazara del Vallo (TP)
- IIS Majorana, Palermo
- IIS Medi, Palermo
- IIS Minutoli, Messina
- Ist. Salesiano Don Bosco-Villa Ranchibile, Palermo
- Istituto Magistrale Regina Margherita, Palermo
- IT Archimede, Catania
- ITE Russo, Paternò (CT)
- ITES A. M. Jaci, Messina
- ITI Marconi, Catania
- ITIS Cannizzaro, Catania
- ITI Vittorio Emanuele III, Palermo
- ITN Caio Duilio, Messina
- Liceo Classico Internazionale Meli, Palermo
- Liceo Classico Umberto I, Palermo
- Liceo De Cosmi, Palermo
- Liceo Scientifico Basile, Palermo
- Liceo Scientifico e Linguistico Umberto di Savoia, Catania
- Liceo Scientifico Fermi, Ragusa
- Liceo Scientifico Galilei, Catania
- Liceo Scientifico Santi Savarino, Partinico (PA)
- Liceo Scientifico Seguenza, Messina
- Liceo Scienze Umane e Linguistico Dolci, Palermo

GARR NEWS - Numero 33
2025 - Semestrale
Registrazione al Tribunale di Roma n. 243/2009 del 21 luglio 2009

Direttore editoriale: Claudia Battista
Direttore responsabile: Gabriella Paolini
Caporedattore: Carlo Volpe
Redazione: Elis Bertazzon, Sara Di Giorgio, Marta Mieli, Erika Trotto
Consulenti alla redazione: Claudio Allocchio, Mauro Campanella, Massimo Carboni, Sabrina Tomassini, Davide Vaghetti, Simona Venuti
Hanno collaborato a questo numero: Claudio Barchesi, Fabrizio Bataloni, Vincenzo Caracciolo, Marco Cirilli, Stefano Claut, Maurizio Davini, Marco Falzetti, Fabio Farina, Eleonora Ferroni, Marco Gallo, Stefano Giordano, Emanuele Guerrini, Alessandro Inzerilli, Leonardo Lanzi, Pasquale Mandato, Giulia Mantovani, Laura Moretti, Martina Po, Gianluigi Spinaci, Stefano Suin, Enrico Venuto, Damiano Verzulli, Giancarlo Viola
Progetto grafico: Carlo Volpe
Impaginazione: Carlo Volpe, Marta Mieli

Editore: Consortium GARR, Via dei Tizii, 6 - 00185 Roma
tel 06 49622000 info@garr.it www.garr.it
ReteGARR

Stampa: Tipografia Grazini e Mecarini
Tiratura: 7.500 copie
Chiuso in redazione: 15 dicembre 2025

Crediti immagini

Immagine di copertina: Istockphoto

Edoardo Angelucci, GARR (pag. 1, 4, 11, 13, 14, 21, 22, 25, 28, 29), Pexels (pag. 2, 17, 19, 23, 25, 35), Unsplash (pag. 9, 33), Ugo Lebreuilly/Progetto Rosetta Stone (pag. 16), Piergiorgio Scarlato e Jacopo Taddeucci (pag. 16), Sparkle (pag. 25), INFN (pag. 25), Sergio Bertani (pag. 39, 40)

I servizi GARR

servizi.garr.it

Rete e accesso

GARR NOC
Gestione della rete

GARR NIC
Nomi a dominio

GARR LIR
Indirizzi IP

Sicurezza informatica

GARR CERT
Gestione e prevenzione

GARR SCARR
Scansioni di vulnerabilità

Identità e mobilità

idem garr aai
Identità digitali

IdP in the cloud
Identity as a Service

GARR CERTIFICATION SERVICE
Certificati digitali

eduroam
Wi-Fi in mobilità

Cloud

GARR cloud
IaaS e object storage

Videoconferenza e streaming

BlueMeet GARR
eduMEET
Soluzioni open per la videoconferenza

GARR TV
Streaming e video

Applicazioni

GARRbox
Storage personale

FILESENDER
Trasferimento file

GARR Mirror
Software Mirror

url GARR
URL brevi

GARR speedtest
Test di connessione

eduVPN
VPN

Hai una storia da condividere?

Scrivici e contribuisci al prossimo numero di GARR News

garrnews.it

garrnews@garr.it

retegarr