CSI
your digital partner

Sovranità digitale

governare dati, infrastrutture e innovazione

DECALOGO

per la sovranità digitale

1. GOVERNA L’IMPIANTO APPLICATIVO E TECNOLOGICO

La gestione diretta di infrastrutture, piattaforme, applicazioni e dati su cui si fondano i servizi digitali è una condizione essenziale per garantire che ogni scelta tecnologica possa essere compresa, verificata e, se necessario, modificata nel tempo.

14.600 server di cui **600** fisici

570 clienti PA su Nivola

30+ pb dati gestiti

2000+ servizi monitorati

2. PUNTA SU STANDARD APERTI

Prima azienda italiana certificata OpenChain

Standard aperti e software open source
sono una condizione essenziale
per ridurre le dipendenze tecnologiche
e rafforzare il controllo pubblico.
Consentono trasparenza, pluralità di fornitori
e crescita delle competenze interne nel tempo.

Su Developers Italia siamo presenti con **79**
tra piattaforme e soluzioni applicative:

- **68** soluzioni applicative
- **9** piattaforme
- **2** soluzioni infrastrutturali

3. RIDUCI L’ESPOSIZIONE DEI DATI A NORMATIVE E ACCESSO DI PAESI TERZI

Dati, informazioni e competenze devono rimanere sotto il controllo tecnico e giuridico dell’Unione Europea. Soluzioni tecnologiche, presìdi giuridici, clausole contrattuali e cooperazione tra enti devono prevenire l’esposizione a regole e accessi non conformi al diritto europeo.
La cifratura è necessaria ma non sufficiente: riservatezza e disponibilità dei dati devono coesistere per garantire sovranità nel tempo.

QI2
Per dati e servizi ORDINARI e CRITICI della PA

QC2
Servizi cloud per dati ORDINARI e CRITICI della PA

CSA STAR Lv. 2 · ANSI TIA Rating III
Cloud Security Alliance + Standard datacenter alta disponibilità

ISO 27001
Sicurezza informazioni

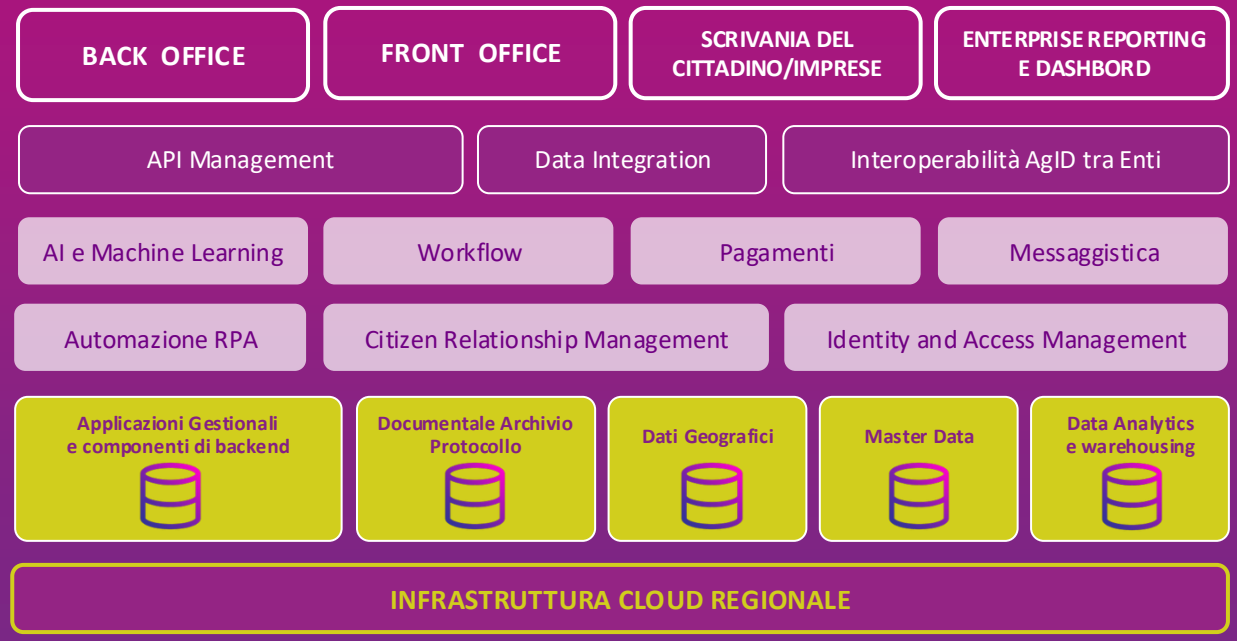
ISO 27017
Sicurezza cloud

ISO 27018
Protezione dati cloud

4. AUMENTA L'INDIPENDENZA TECNOLOGICA

Le applicazioni e le piattaforme della pubblica amministrazione devono essere progettate per evolvere nel tempo senza compromettere l'intero sistema.
Modularità e interoperabilità evitano dipendenze irreversibili e preservano la libertà di scelta.

Abbiamo costruito i sistemi informativi dei nostri Enti secondo i principi della composable architecture



5. PROMUOVI UNA AI RESPONSABILE

Le soluzioni di AI nella PA devono essere progettate in modo trasparente e controllabile. Separare dati, modelli e processi decisionali consente di mantenere il controllo pubblico, garantire conformità normativa e ridurre dipendenze tecnologiche, costituendo una condizione abilitante per la sovranità digitale.

- **Policy di utilizzo degli strumenti di GenAI**
- **Corsi di formazione interna per utilizzo consapevole AI**
- **Checklist livello di rischio progetti AI per gli enti sulla base dell'AI act**
- **Sicurezza strutturale**
- **Governance e supervisione**
- **Minimizzazione e isolamento**
- **Miglioramento continuo governato**

6. INVESTI IN FORMAZIONE

DIGITALCAMPUS
guidiamo l'innovazione

È fondamentale poter disporre di personale interno con competenze tecniche su cybersecurity, AI e cloud sempre aggiornate per mantenere la conoscenza e il controllo diretto delle soluzioni adottate.

FORMAZIONE ESTERNA

circa **138** corsi erogati

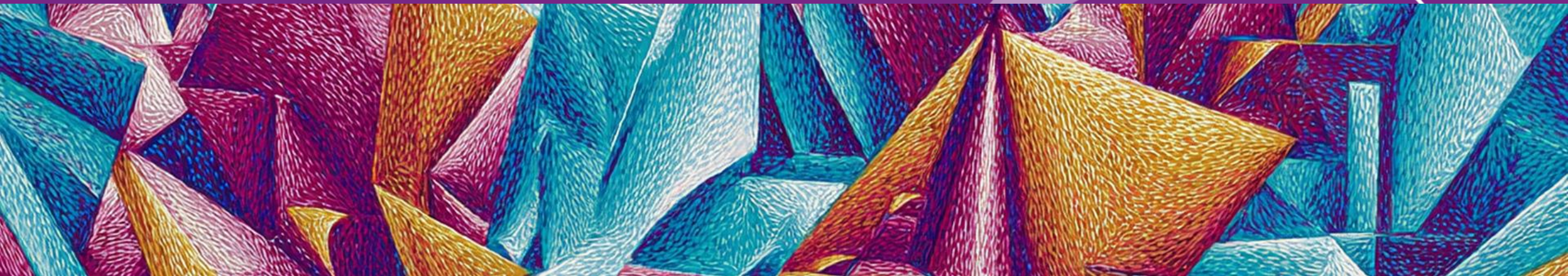
circa **40mila** partecipanti alla formazione

FORMAZIONE INTERNA

3.000+ giorni annui di formazione

7. GARANTISCI DISPONIBILITÀ, RESILIENZA E CONTINUITÀ OPERATIVA

Le infrastrutture pubbliche devono essere progettate per garantire affidabilità e continuità nel tempo.
Ridondanza, distribuzione e controllo delle infrastrutture e dei servizi permettono di assicurare prestazioni stabili e resilienza anche in condizioni critiche.



8. GOVERNA L’USO DEI DATI DELLA PUBBLICA AMMINISTRAZIONE

Conoscere e classificare i propri asset digitali
è una condizione essenziale per un uso corretto
dei dati. Apertura, tutela e utilizzo dei dati,
anche per AI e ricerca, devono essere
sempre orientati all’interesse pubblico.

FASCICOLO SANITARIO Elettronico

certificato **ISDP10003**
conformità dei processi relativi ai trattamenti
di raccolta, gestione, consultazione
e archiviazione di dati personali e particolari
per il Fascicolo Sanitario Elettronico

Applicazione integrale direttiva NIS 2 relativa ai servizi essenziali

7.108 **dipendenti di PA e atenei** hanno fatto
formazione su phishing e cybersecurity nel 2025

Soggetto essenziale NIS 2
in quanto Cloud Service Provider

9. PUNTA ALLA MASSIMA CONDIVISIONE

Condividere competenze, riusare software
e mettere in rete le esperienze evita duplicazioni
e moltiplica il valore degli investimenti pubblici.
La collaborazione, fondata su standard comuni,
altruismo dei dati e cloud federato,
trasforma risultati locali in un ecosistema
pubblico, interoperabile e sovrano.

Open data

1.563 dataset

Geoportale Piemonte

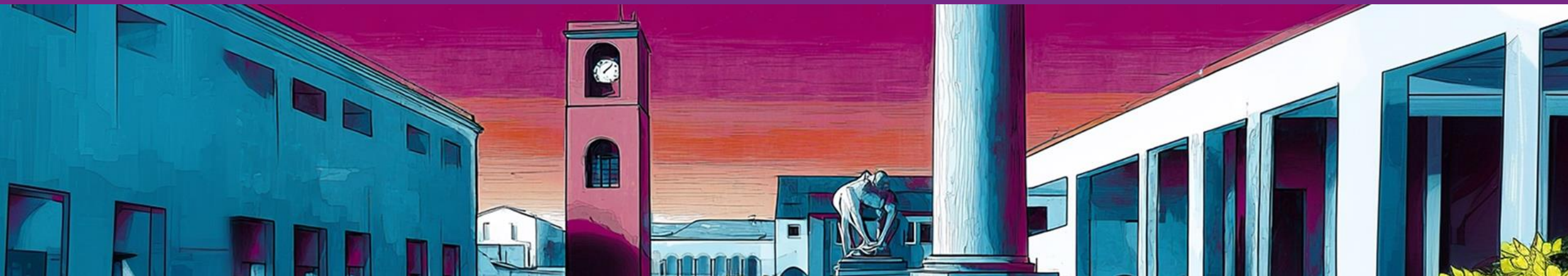
2.200.000

edifici rappresentati nella nostra
infrastruttura geografica regionale

ASSINTERITALIA

Esperienza **Assinter**
per la condivisione delle
competenze tra in house

Accordi di collaborazione tra
in house con **Liguria Digitale**
e **ACI Informatica** in progetti legati
a cloud, sicurezza e observability



10. ORIENTA OGNI DECISIONE TECNOLOGICA A VANTAGGIO DEL BENE COMUNE

Le scelte tecnologiche della pubblica amministrazione devono essere orientate al bene collettivo, alla tutela dei diritti dei cittadini e alla sostenibilità nel tempo.

CSI
your digital partner