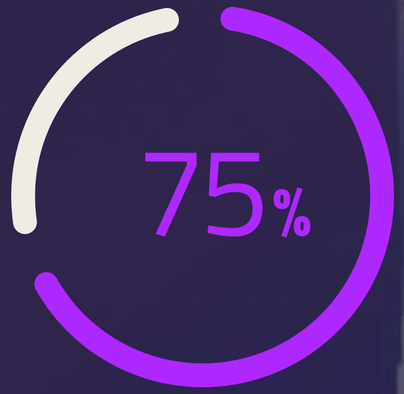
Platform

Infrastrutture e sicurezza
al servizio dell’innovazione

IC
InfoCamere

Platform - Infrastrutture e Sicurezza a servizio dell'innovazione

Garanzia della business continuity



Supporto all'innovazione, alla ricerca e alla digitalizzazione

Tutela della privacy e sicurezza dei dati

SDGs

Platform

Un cuore pulsante che mette in circolo l'innovazione: con infrastrutture in costante evoluzione che garantiscono elevati livelli di sicurezza, il Gruppo InfoCamere realizza e gestisce, per conto del Sistema Camerale, infrastrutture strategiche nazionali a servizio dell'innovazione condivisa con le altre Pubbliche Amministrazioni ed il sistema imprenditoriale italiano.

Infrastrutture e Sicurezza a servizio dell'innovazione

HIGHLIGHTS

Evoluzione delle infrastrutture tecnologiche

Investimenti in innovazione 8,39 mln

Cyber security:

- Verso la **certificazione ISO 27701:2019**
- Effettuati interventi di **compliance alla direttiva NIS2**

Infrastrutture innovative

ALCUNI NUMERI SULLE INFRASTRUTTURE DEL GRUPPO INFOCAMERE

La server farm custode del patrimonio informativo del Sistema Camerale italiano

DATA CENTER INFOCAMERE

- Il Gruppo InfoCamere gestisce il patrimonio informativo del Sistema Camerale Italiano attraverso il Data Center di Padova ed una rete infrastrutturale che unisce tutte le Camere di Commercio Italiane
- Un secondo Data Center funziona come secondo access point di rete e come Disaster Recovery Center
- I servizi sono erogati in continuità operativa grazie all'infrastruttura di Continuous Availability
- Il Data Center è l'hub di accesso al patrimonio informativo, aggiornato in tempo reale, del tessuto imprenditoriale, economico e produttivo italiano.

SICUREZZA, ALTA AFFIDABILITÀ, TECNOLOGIA

- Sistema antincendio a gas ecologico (IG-541)
- Controlli perimetrali e delle aree interne sensibili quali il Data Center e le aree pertinenziali
- Infrastruttura elettrica ridondata: doppia alimentazione per tutti gli apparati
- Potenza complessiva: isole ad alta densità, progettate per supportare una potenza di 500 KW, pari al consumo di 300 famiglie, ospitate in un'area di dimensioni di un campo di basket
- Apparati di rete e server di ultima generazione, oltre 550 Data Base gestiti e 3.800 server tra fisici e virtuali con un'elevata virtualizzazione dei sistemi (96%)
- Sistemi storage: capacità oltre 14.000 TB corrispondenti a 28 milioni di libri digitalizzati che impilati l'uno sull'altro raggiungono 600 km di altezza

SALA CONTROLLO

- Presidio H24 per 365 giorni da parte di personale in turnazione
- Oltre 61.000 controlli infrastrutturali (Server, Storage e Networking)
- Oltre 8.000 controlli ambientali (temperatura, umidità e assorbimento elettrico)
- Oltre 160.000 simulazioni automatiche al giorno monitorano i tempi di risposta e la disponibilità dei servizi
- Circa 60.000 elaborazioni giornaliere governate dai sistemi di schedulazione automatica riducono l'intervento umano
- Oltre 2.500 applicazioni gestite
- Oltre 837 interventi infrastrutturali nell'ultimo anno
- Circa 6.600 rilasci software in produzione
- Presidio del processo di Incident & Problem Management secondo lo standard ISO 20000 e Best Practices ITIL quale garanzia di continuità operativa e continuo miglioramento

CERTIFICAZIONI

- ISO 9001 Qualità
- ISO 20000-1 Servizi IT
- ISO 22301 Continuità Operativa
- ISO 25012 Qualità Dati Registro Imprese
- ISO 27001 Sicurezza informazioni:
- 27017 Sicurezza in Cloud
- 27018 Privacy in Cloud
- ISO 14001 Ambientale
- EMAS
- Dichiarazione Ambientale
- eIDAS Prestatore Servizi Fiduciari Qualificati
- eIDAS Prestatore Servizi Fiduciari SPID
- Industria 4.0 Centro per il trasferimento tecnologico
- STANDARD DI ESERCIZIO DATA CENTER - ANSI/TIA 942-C-2024 Rating 3

Il cuore pulsante di questa infrastruttura è il Data Center di Padova, un sito progettato secondo i più rigorosi standard di sostenibilità, affidabilità e sicurezza. Operando in regime di Continuous Availability, l'infrastruttura assicura risposte immediate e in continuità a cittadini, imprese e Pubblica Amministrazione, gestendo volumi critici:

- oltre 3.800 sistemi fisici e virtuali;
- oltre 14.000 Terabyte (TB) di dati;
- traffico di 15,4 TB sulla rete camerale e 27,2 TB su Internet;
- 150.000 controlli giornalieri, con un totale annuo stimato di 32 miliardi di operazioni.

L'eccellenza operativa è attestata dal possesso di "Standard di esercizio Data Center - ANSI/TIA 942-C-2024 Rating 3, da ultimo rinnovata nel corso del 2025, che costituisce requisito primario per mantenere l'accreditamento recentemente ottenuto da ACN come soggetto abilitato ad erogare servizi Cloud per la PA.

Business continuity. il Gruppo InfoCamere eroga servizi in continuità operativa secondo lo standard ISO 22301. Il Data Center è protetto da eventi di interruzione elettrica mediante gruppi di continuità (UPS) e gruppi elettrogeni che garantiscono autonomia di funzionamento per più giorni. Le infrastrutture elettriche, di raffreddamento e di networking, sono ridondate: per tutti gli apparati è prevista una doppia alimentazione attraverso due distinti rami. Questo garantisce la possibilità di intervenire in qualunque parte dell'impianto senza causare interruzioni del servizio. Analoga strategia è implementata per i collegamenti di rete geografici.

Disaster Recovery. un secondo Data Center funge da access point secondario e Disaster Recovery Center. È interconnesso con la sede di Padova tramite linee in fibra ottica 10 Gigabit Ethernet con doppio operatore, garantendo elevata affidabilità.

Di seguito alcuni indicatori di disponibilità e continuità di erogazione dei servizi degli ultimi tre anni misurati in rapporto al totale del tempo di erogazione previsto.

DISPONIBILITÀ E CONTINUITÀ DI EROGAZIONE DI TUTTI I SERVIZI

2025 **2024** **2023**

Salvaguardia del patrimonio informativo

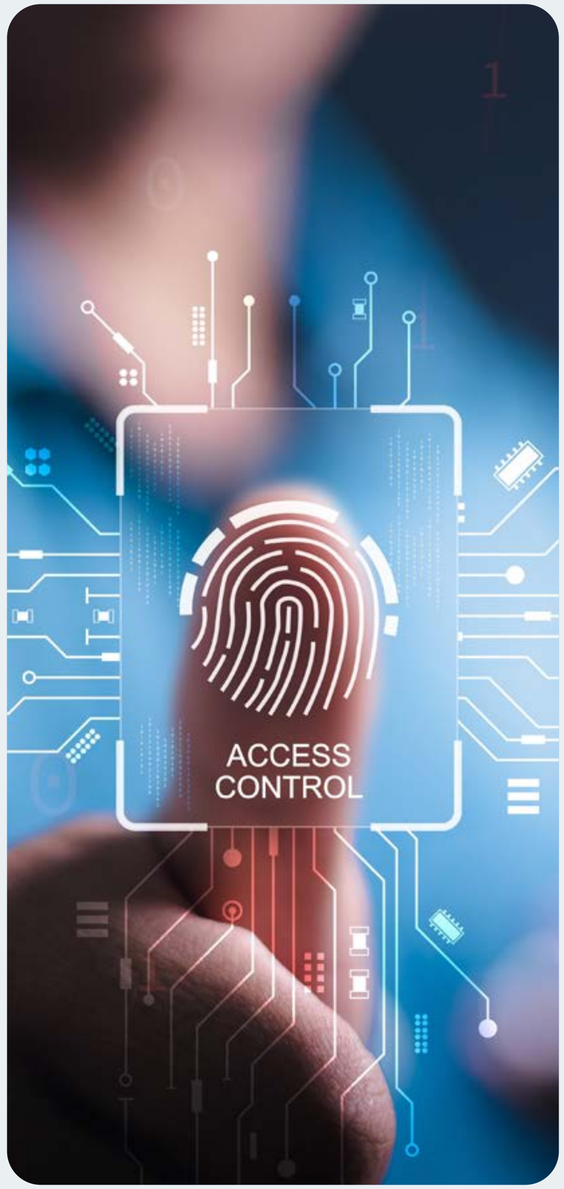
Protezione dell'infrastruttura: sicurezza fisica e logica

Per garantire la massima protezione delle infrastrutture, nel Data Center di InfoCamere sono adottati avanzati sistemi di sicurezza sia per il controllo degli accessi sia per la prevenzione di incendi e altri rischi operativi. La sicurezza è garantita attraverso un sofisticato sistema di monitoraggio, che copre sia l'ambiente esterno che le aree interne del Data Center:

- difesa del perimetro esterno: l'intero complesso è circondato da una recinzione di sicurezza e costantemente sorvegliato tramite un sistema di videosorveglianza con telecamere (TVCC) dotate di analisi video avanzata. Inoltre, un team di sicurezza è presente 24 ore su 24 per controllare l'edificio e gestire gli accessi alle aree sensibili;
- monitoraggio delle aree interne: per garantire una protezione efficace anche all'interno della struttura, sono stati installati rivelatori combinati a microonde e infrarossi, capaci di individuare qualsiasi movimento sospetto. La gestione di tutti questi dispositivi è affidata a una centrale antintrusione, che non solo monitora costantemente il sistema ma segnala immediatamente eventuali anomalie o malfunzionamenti.

Nel complesso, la struttura dispone di un sistema di supervisione all'avanguardia, che attraverso circa 8.000 sensori monitora costantemente i principali parametri di funzionamento, tra cui la presenza di incendi, tentativi di intrusione, variazioni di temperatura e umidità, oltre ai livelli di assorbimento elettrico.
Per garantire la sicurezza logica, le reti aziendali sono protette da firewall a più livelli per gestire le diverse aree di criticità e da sistemi di Intrusion Prevention (IPS) e Anti-DDoS (Distributed Denial of Service). Le principali misure di sicurezza tecnologica comprendono antivirus e antimalware su tutti i sistemi, la gestione e il backup dei dati e la registrazione delle attività di sistema (log). Tra le misure di sicurezza è di particolare importanza la procedura di Disaster Recovery testata ogni anno.

Per assicurare la protezione dei sistemi informativi aziendali, InfoCamere si avvale di un proprio Security Operation Center (SOC), parte integrante della struttura organizzativa "Technology Infrastructure & Security Operation". Il SOC è composto da personale interno ed esterno, in costante contatto con organismi di early-warning: que



sto consente al Gruppo di essere più tempestivo ed efficace sia nella prevenzione degli attacchi informatici sia nella reazione in caso di incidente. In particolare, Il SOC opera attraverso un modello di sicurezza integrato su tre livelli:

- sicurezza proattiva: analizza costantemente i sistemi e implementa le difese necessarie per prevenire attacchi informatici;
- sicurezza reattiva: monitora le attività in tempo reale e interviene rapidamente per gestire eventuali incidenti di sicurezza;
- sicurezza predittiva: sfrutta strumenti avanzati di threat intelligence per individuare potenziali minacce e predisporre strategie di difesa prima che si verifichino.

Oltre alle attività operative, la divisione Technology Infrastructure & Security Operation promuove iniziative di sensibilizzazione e formazione sulla sicurezza informatica per i dipendenti, oltre a fornire supporto consulenziale alle diverse aree aziendali nei progetti che richiedono elevati standard di protezione dei dati.

Protezione del patrimonio informativo: sistema di gestione sicurezza delle informazioni e privacy

Parallelamente alla protezione delle infrastrutture, costante è l'impegno del Gruppo per preservare la riservatezza, l'integrità e la disponibilità del patrimonio informativo.

A tal fine, InfoCamere adotta un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) certificato dal 2012 secondo lo standard ISO/IEC 27001. Nel 2019 ha esteso la certificazione anche al Cloud-Computing[10], ottenendo la conformità agli standard ISO/IEC 27017 e ISO/IEC 27018. Il modello SGSI definisce l'organizzazione del sistema, le procedure interne e l'analisi dei rischi di sicurezza; inoltre stabilisce le politiche di sicurezza che coprono aspetti organizzativi e tecnologici (es. gestione degli incidenti, controlli di accesso, ecc.). Tutti i dipendenti sono chiamati al rispetto delle politiche di sicurezza che si estendono a tutti i processi aziendali.
È in vigore una Politica e un processo specifico per la protezione dei dati che InfoCamere gestisce come Titolare o Responsabile del trattamento per conto delle Camere di Commercio e/o di altri Enti, in conformità al Regolamento Europeo 2016/679 (GDPR). Inoltre, è stata definita una procedura ad hoc in caso di Data Breach, (violazione dei dati personali) come previsto dagli articoli 33 e 34 del GDPR.

Negli ultimi anni è stata intensificata la formazione del personale, sono state aggiornate le procedure per documentare le caratteristiche di sicurezza e privacy dei sistemi informativi gestiti ed è stato inoltre sviluppato un servizio per la gestione del Registro dei Trattamenti.

Il processo attivo per la gestione dei reclami non ha rilevato, nell'ultimo triennio, alcuna richiesta concernente violazioni della privacy o per perdite di dati.

[10] InfoCamere ha predisposto specifiche politiche di sicurezza che disciplinano regole da applicare in ambito Cloud Computing impegnandosi per operare costantemente in conformità con la normativa vigente sul tema. Nel corso del 2024 InfoCamere ha concluso il percorso di qualificazione presso ACN della propria infrastruttura per l'erogazione di servizi cloud che trattano dati di livello ordinario e critico.

Evoluzione dell’infrastruttura, sicurezza, innovazione tecnologica

Innovazione tecnologica ed evoluzione dell’infrastruttura

Il 2025 ha segnato un punto di svolta per le infrastrutture del Gruppo. Gli interventi effettuati non hanno riguardato semplici aggiornamenti tecnologici, ma il consolidamento di un ecosistema digitale reattivo, capace di supportare la missione del Gruppo in un panorama normativo complesso e segnato da crescenti minacce cyber. Numerose sono state le attività correttive ed evolutive per ottimizzare le risorse, massimizzare le prestazioni e garantire adeguati livelli di sicurezza. L'intensa attività di trasformazione — caratterizzata da oltre 800 interventi correttivi ed evolutivi — non ha avuto alcun impatto sul livello di servizio generale che nel 2025 si è mantenuto pari al 99,95%.

Per massimizzare il **controllo e le prestazioni dell’infrastruttura**, sono state compiute scelte strategiche mirate all'efficienza, con upgrade tecnologici che garantiscono una gestione dei carichi più fluida e scalabile; il passaggio a nuovi modelli infrastrutturali ha consentito di recuperare potenza di calcolo, abbattere la latenza e ottimizzare i costi.

Nell’ambito della **valorizzazione del patrimonio informativo**, è stata sviluppata la componente tecnologica del progetto “Centrale Eventi” che, grazie all'introduzione di processi Data-Driven, ha la capacità di reagire in tempo reale alle variazioni dei dati, abilitando decisioni rapide e servizi applicativi proattivi e integrati.

Relativamente alla **Cyber Resilienza** e **Trust Digitale** la sicurezza si è evoluta a fattore abilitante che migliora il servizio; la strategia di difesa adottata agisce su più livelli e in modo anticipato, poggiando su tre pilastri fondamentali:

- protezione esterna e applicativa: l'installazione di firewall di nuova generazione e scudi specifici per le Web Application mitiga l'esposizione dei servizi agli attacchi più sofisticati;
- ricerca e analisi delle minacce: sistemi intelligenti analizzano costantemente enormi volumi di dati individuando minacce reali e neutralizzandole rapidamente, riducendo drasticamente i tempi di reazione e ripristino;
- data protection: i sistemi di backup sono stati potenziati con tecnologie moderne che creano copie sicure e immutabili, garantendo un ripristino dei servizi rapido e affidabile.

L'evoluzione del 2025 ha raggiunto anche le sedi locali delle Camere di Commercio con l'ammodernamento delle reti LAN e l'installazione di oltre 160 nuovi punti di accesso WiFi; tali interventi hanno potenziato l'agilità operativa e la connettività di tutto il sistema.

Standard e innovazione delle architetture applicative

Nel 2025 sono state avviate diverse iniziative di innovazione tecnologica, tra cui: percorsi di formazione avanzata su piattaforme workspace, la sperimentazione dell'intelligenza artificiale generativa, l'implementazione di soluzioni di intelligent automation per la creazione di una "Digital Workforce" finalizzata all'automazione di attività ripetitive, e la verifica di un'infrastruttura VoIP in ambiente cloud per potenziare la comunicazione e la collaborazione in mobilità.

Le sperimentazioni condotte si sono concluse con esito positivo, confermando la validità delle soluzioni analizzate e la loro coerenza con gli obiettivi di evoluzione tecnologica ed efficientamento operativo. I risultati conseguiti costituiranno la base per le future scelte strategiche aziendali.

Valorizzazione spazi tecnologici ed efficientamento energetico

Nell'ambito degli interventi volti a migliorare l'efficienza e l'affidabilità delle infrastrutture, nel corso del 2025 InfoCamere ha completato attività cruciali nel percorso verso soluzioni che coniughino massima capacità operativa, contenimento dei costi energetici e sostenibilità ambientale.

Presso la sede di Padova, è stato ultimato il potenziamento del Data Center primario, raggiungendo una capacità IT di 1 MW. Parallelamente, è stato avviato il progetto di ampliamento di un nuovo ambiente tecnologico che ha già visto la conclusione dello strip-out dei locali e la realizzazione strutturale del nuovo avancorpo d'accesso. Questi spazi fisici ospiteranno impianti indipendenti in grado di garantire ulteriori 500 kW di carico.

Il nuovo assetto impiantistico non solo potenzia le capacità interne, ma abilita l'offerta di servizi avanzati di colocation, garantendo a terze parti i medesimi standard di continuità operativa, elettrica e di raffreddamento delle infrastrutture proprietarie. Questo impegno tecnologico si riflette anche sull'impronta energetica: gli interventi di ammodernamento e ampliamento del Data Center e degli uffici porteranno a un risparmio stimato di circa 80.000 kWh/anno, consolidando l'approccio orientato all'efficienza e alla responsabilità ambientale.

Cybersecurity: salvaguardia del patrimonio informativo

Nel 2025 è stato mantenuto alto il presidio in cybersecurity, che ha consentito:

i) il completamento degli adempimenti normativi per la compliance alla direttiva NIS2;

ii) la conclusione delle attività propedeutiche all'ottenimento della certificazione ISO 27701 sulla gestione delle informazioni e privacy.

In particolare, con riferimento alla NIS2 sono state completate le comunicazioni obbligatorie verso le autorità competenti, con la nomina del Referente CSIRT (*Computer Security Incident Response Team*) e sono state aggiornate le procedure interne per la gestione degli incidenti e delle vulnerabilità informatiche.

Particolare attenzione è stata inoltre dedicata alla governance dell'Intelligenza Artificiale: nel corso dell'anno sono stati avviati i lavori per la definizione di policy e requisiti volti a vigilare sulla piena conformità normativa e di sicurezza nello sviluppo e nell'approvvigionamento di soluzioni basate su IA.

Di seguito le principali iniziative portate avanti nel 2025 per affinare nel continuo le capacità di difesa così da consentire il rafforzamento strategico della postura di cybersecurity:

- Potenziamento delle tecnologie di difesa: per ridurre i tempi di reazione e aumentare la precisione degli interventi, sono state potenziate le tecnologie di monitoraggio ottimizzando i Playbook XDR per risposte differenziate in base alla criticità degli asset. Parallelamente, l'aggiornamento di Cisco CES ha rafforzato la protezione contro il phishing, principale vettore d'attacco.
- Cyber Threat Intelligence e Osservabilità: è proseguita l'integrazione avanzata tra le piattaforme di Threat Intelligence (MISP) e i sistemi di difesa perimetrale (Splunk, IPS), trasformando i segnali di minaccia esterni in regole di difesa automatizzate. In parallelo, è stata potenziata la capacità di "osservabilità" dei sistemi ibridi estendendo la raccolta di log su Google Cloud Platform (GCP) e sui nuovi firewall, garantendo una visione unitaria della sicurezza tra ambienti on-premise e cloud.
- Verifica della sicurezza (*Vulnerability & Penetration Testing*): durante l'anno sono stati condotti numerosi test di sicurezza su applicazioni e infrastrutture critiche. In particolare, test intensivi (Vulnerability & Penetration Testing) sono stati condotti su asset strategici. Queste attività sono fondamentali per risolvere preventivamente le vulnerabilità e mantenere i massimi standard di certificazione (SPID, QTSP, ISO27001).

Sinergia per lo sviluppo delle infrastrutture digitali della Pubblica Amministrazione: la collaborazione tra InfoCamere S.C.p.A. e CINECA – Consorzio Interuniversitario

Nel corso del 2025 il Gruppo InfoCamere ha sottoscritto un accordo di collaborazione con CINECA, società in house del sistema universitario e della ricerca pubblica italiana, che abilita la condivisione reciproca di specifiche aree dei propri Data Center, insieme ad una serie di facility e di attività funzionali, volta ad assicurare e rafforzare le rispettive procedure di sicurezza e continuità operativa.

InfoCamere e CINECA operano quali organismi in house rispettivamente delle Camere di Commercio e del sistema universitario e della ricerca pubblica italiana; entrambe sono dotate di infrastrutture digitali conformi ai requisiti stabiliti dall'Agenzia per la Cybersicurezza Nazionale (ACN) per garantire elevati standard di sicurezza, disponibilità e resilienza. La Collaborazione realizza l'obiettivo comune di rafforzare la postura di sicurezza e resilienza, in linea con le normative di settore nazionali, rendendo le rispettive infrastrutture digitali sempre più sicure ed affidabili, in coerenza ed attuazione della missione istituzionale di InfoCamere. L'obiettivo è quello di evolvere reciprocamente i piani di emergenza di entrambe le società per assicurare la continuità operativa e il rapido ripristino dei servizi informatici essenziali e, allo stesso tempo, contribuire a rendere le infrastrutture e i servizi digitali della Pubblica Amministrazione sempre più sicuri e affidabili, in linea con le disposizioni normative e regolamentari vigenti.

La Collaborazione si fonda su un principio di piena reciprocità prevedendo, in particolare:

- la messa a disposizione di servizi infrastrutturali, che consistono nella condivisione reciproca di specifiche aree di data center, unitamente ad una serie di facility e di attività funzionali volte ad assicurare e rafforzare la Disaster Recovery;
- un progetto comune per l'evoluzione della continuità operativa: entrambe le parti mettono a disposizione il proprio know-how, le best practice e le esperienze maturate per individuare e valutare la fattibilità di ulteriori e più avanzate soluzioni di continuità operativa.

Con tali premesse si intendono perseguire molteplici benefici per InfoCamere, quali:

- incremento della resilienza: l'utilizzo reciproco dei data center aumenta la capacità di Disaster Recovery, rafforzando la continuità operativa dei servizi critici.
- ottimizzazione dei costi: sfruttare le infrastrutture esistenti di entrambe permette di realizzare efficientamenti e economie di scala, conseguendo benefici operativi ed economici.
- innovazione: la collaborazione nel progetto congiunto consente di esplorare e potenzialmente implementare soluzioni avanzate di business continuity.
- rafforzamento delle competenze: la condivisione di esperienze e know how contribuisce alla crescita professionale e tecnologica interna.

I servizi IT a servizio del Sistema Camerale e delle altre istituzioni

Il Gruppo InfoCamere offre ai propri Soci, nel rispetto di quanto previsto dal TUSP, un ventaglio di servizi IT caratterizzati dalla flessibilità offerta e dall'assistenza garantita. Tutte le soluzioni proposte prevedono anche servizi di supporto, backup, monitoraggio e presidio organizzati in processi aderenti alle Best Practices ITIL e conformi ai Requisiti della Certificazione ISO/IEC 20000-1.
Di seguito un dettaglio dei servizi IT disponibili:

Servizio di *housing* per i Data Center e relativa estensione: offerta di servizi di colocation per ospitare le infrastrutture di soggetti istituzionali che optano per esternalizzare il Data Center. L'estensione o la colocation del Data Center consente, sfruttando le tecnologie più innovative e le esperienze maturate nel campo, di applicare soluzioni in grado di propagare reti ed infrastrutture (c.d. Cloud ibrido), garantendo efficienza e continuità dei servizi.

Virtual Data Center: Il servizio Private Cloud mette a disposizione risorse computazionali (CPU, RAM e Spazio Disco) e di networking prevedendo diverse tipologie di Hypervisor di sistema operativo e di piattaforme Middleware.

Hosting: I servizi di hosting di sistemi e applicazioni, anche in qualità di internet service provider, consentono di ospitare ambienti di tutte le complessità, da architetture Mission Critical ai siti web e agli ambienti di sviluppo.
Continuità operativa: Le proposte di Disaster Recovery e continuous availability prevedono l'automazione di processi di replica di Virtual Data Center completi o di singole macchine virtuali, assicurando RPO e RTO ridotti.

Servizio di VDI: Il servizio VDI (Virtual Desktop Infrastructure) ospita 3.650 Desktop Virtuali all'interno dei Data Center InfoCamere (modalità SaaS). Il numero di VDI può essere facilmente e rapidamente aumentato a fronte di nuove richieste. La soluzione offerta prevede l'erogazione di desktop di ultima generazione, con CPU, memoria ed applicazioni personalizzabili in base alle esigenze.