2

Allegato

Documento Strategie ICT

nelle more del Piano Triennale
per l'Informatica dell'Ateneo di Firenze

Indice

1 Governance al digitale

Lo sviluppo dei sistemi informativi è diventato un punto fondamentale a garanzia del corretto funzionamento dei processi all'interno delle organizzazioni. Le particolari condizioni organizzative e la continua necessità di modificare i processi interni ha bisogno di un'architettura dei sistemi informativi particolarmente flessibile e quindi capace di dare risposte veloci ed efficaci alle necessità dei processi.

L'Ateneo di Firenze ha iniziato già dal 2017 un percorso di riorganizzazione interna che si è concretizzato con la definizione di una Funzione Trasversale dedicata all' "Innovazione per lo sviluppo sinergico dei processi di informatizzazione dell'Ateneo" e la creazione del "Area per l'Innovazione e Gestione dei Sistemi informativi ed Informatici" con la finalità di favorire e rendere pienamente operative, oltre che sinergiche, le strutture interne armonizzando gli apporti dati da ciascuno all'evoluzione dei sistemi e degli strumenti informatici nell'ottica di una loro progettazione unitaria, di ampia e capillare diffusione.
Insieme ai dipartimenti DISIA e DINFO costituisce la Piattaforma di Innovazione per lo sviluppo dei processi di informatizzazione dell'Ateneo e definisce le strategie di evoluzione dell'architettura tecnologica dell'Ateneo.

L'Area per l'Innovazione e Gestione dei Sistemi informativi ed Informatici include una struttura chiave di supporto all'innovazione "EAPMO (Enterprise Architecture & Project Management Office)" dedicata alle attività di pianificazione e monitoraggio nell'ambito della Funzione Trasversale.

Le attività prevalenti di EAPMO riguardano:

- Supporto operativo e metodologico alla gestione e governo dei progetti e dei processi anche tramite l'individuazione delle metodologie e strumenti di PM da utilizzare
- Promozione e aggiornamento di metodologie di project management e relativa formazione
- Valutazione tecnica delle soluzioni interne ed esterne più adatte a soddisfare le esigenze espresse dalla cabina di regia nell'ambito della funzione trasversale
- Garanzia della coerenza delle nuove iniziative con il percorso di evoluzione organizzativa e tecnologica dei sistemi informativi e allineamento agli obiettivi strategici di Ateneo
- Monitoraggio delle attività dell'ambito verificando il rispetto della pianificazione ed il coordinamento con gli altri settori
- Coordinamento delle attività nell'ambito della qualità e sicurezza informatica
- Promozione della partecipazione dell'Area e della Funzione Trasversale a progetti di ricerca e collaborazione nazionale e internazionale
- Definizione delle priorità di azione in base alle indicazioni della cabina di regia e il Front Office SIAF ed in collaborazione con le altre strutture dell'Ateneo
- Attività di raccolta e catalogazione delle informazioni prodotte dall'insieme dei progetti tecnologici di Ateneo
- Il monitoraggio e la diffusione dei progressi relativi al percorso di evoluzione tecnologica dell'Ateneo

Sotto il coordinamento della cabina di regia della funzione trasversale il gruppo EAPMO fornisce supporto operativo con l'obiettivo di una migliore gestione complessiva dei servizi orientata non solo alla produzione di applicativi di qualità, ma con particolare attenzione alla capacità di fornire nel tempo la necessaria manutenzione correttiva, normativa ed evolutiva.
Queste attività non possono prescindere dalla collaborazione con altre strutture e pertanto si intende attivare gruppi di sviluppo multidisciplinari che siano in grado di gestire con modalità standardizzate l'intero ciclo di vita dell'applicativo.
Il gruppo di Enterprise Architecture ha anche il ruolo di assicurare la compatibilità tra quanto prodotto con tutta l'architettura dei sistemi informativi orientando opportunamente le scelte progettuali.

Anche al livello nazionale si assiste ad un'accelerazione delle azioni a sostegno della digitalizzazione della Pubblica Amministrazione probabilmente incoraggiata anche dai pessimi risultati dell'ultimo Europe's Digital Progress report del 2017 che vede l'Italia al quartultimo posto in Europa. Tale processo viene fortemente sostenuto anche a livello politico sia tramite il potenziamento dell'Agenzia per L'italia Digitale (AGID) sia tramite modifiche e aggiornamenti della normativa in vigore. Inoltre, l'Ateneo ha iniziato già dal 2017 un percorso di riorganizzazione del settore informatico

Ad avere impatto diretto sulle Pubbliche Amministrazioni è sicuramente il Decreto Legislativo 7 marzo 2005, n. 82 Codice dell'amministrazione digitale – CAD (aggiornato al decreto legislativo 13 dicembre 2017, n. 217) che prevedeva una serie di misure dedicate alla digitalizzazione già dalle prime versioni ma che vengono rinforzate in modo rilevante nell'ultimo aggiornamento in particolare tramite l'art. 17 che introduce la figura del Responsabile per la Transizione al Digitale (RTD).

I compiti del RTD sono articolati in 10 punti:
a) coordinamento strategico dello sviluppo dei sistemi informativi, di telecomunicazione e fonia, in modo da assicurare anche la coerenza con gli standard tecnici e organizzativi comuni;
b) indirizzo e coordinamento dello sviluppo dei servizi, sia interni che esterni, forniti dai sistemi informativi di telecomunicazione e fonia dell'amministrazione;
c) indirizzo, pianificazione, coordinamento e monitoraggio della sicurezza informatica relativamente ai dati, ai sistemi e alle infrastrutture anche in relazione al sistema pubblico di connettività, nel rispetto delle regole tecniche di cui all'articolo 51, comma 1;
d) accesso dei soggetti disabili agli strumenti informatici e promozione dell'accessibilità anche in attuazione di quanto previsto dalla legge 9 gennaio 2004, n. 4;
e) analisi periodica della coerenza tra l'organizzazione dell'amministrazione e l'utilizzo delle tecnologie dell'informazione e della comunicazione, al fine di migliorare la soddisfazione dell'utenza e la qualità dei servizi nonché di ridurre i tempi e i costi dell'azione amministrativa;
f) cooperazione alla revisione della riorganizzazione dell'amministrazione ai fini di cui alla lettera e);
g) indirizzo, coordinamento e monitoraggio della pianificazione prevista per lo sviluppo e la gestione dei sistemi informativi di telecomunicazione e fonia;
h) progettazione e coordinamento delle iniziative rilevanti ai fini di una più efficace erogazione di servizi in rete a soggetti giuridici mediante gli strumenti della cooperazione applicativa tra pubbliche amministrazioni, ivi inclusa la predisposizione e l'attuazione di accordi di servizio tra amministrazioni per la realizzazione e compartecipazione dei sistemi informativi cooperativi;
i) promozione delle iniziative attinenti l'attuazione delle direttive impartite dal Presidente del Consiglio dei Ministri o dal Ministro delegato per l'innovazione e le tecnologie;
j) pianificazione e coordinamento del processo di diffusione, all'interno dell'amministrazione, dei sistemi di identità e domicilio digitale, posta elettronica, protocollo informatico, firma digitale o firma elettronica qualificata e mandato informatico, e delle norme in materia di accessibilità e fruibilità nonché del processo di integrazione e interoperabilità tra i sistemi e servizi dell'amministrazione e quello di cui all'articolo 64-bis;

j-bis) pianificazione e coordinamento degli acquisti di soluzioni e sistemi informatici, telematici e di telecomunicazione al fine di garantirne la compatibilità con gli obiettivi di attuazione dell'agenda digitale e, in particolare, con quelli stabiliti nel piano triennale di cui all'articolo 16, comma 1, lettera b).

Sempre a livello nazionale si è estremamente rilevante il Piano triennale per l'Informatica nella Pubblica Amministrazione che è il documento di indirizzo strategico ed economico destinato a tutta la Pubblica Amministrazione che accompagna la trasformazione digitale del Paese. Il Piano definisce le linee operative di sviluppo dell'informatica pubblica; il Modello strategico di evoluzione del sistema informativo della PA; gli investimenti ICT del settore pubblico secondo le linee guida europee e del Governo.

L'articolo 17 del CAD prevede che ogni pubblica amministrazione, per garantire l'attuazione delle linee strategiche per la riorganizzazione e la digitalizzazione dell'amministrazione definite dal Governo, "affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale e i conseguenti processi di riorganizzazione finalizzati alla realizzazione di un'amministrazione digitale e aperta, di servizi facilmente utilizzabili e di qualità, attraverso una maggiore efficienza ed economicità". Il Responsabile della transizione al digitale è la figura preposta alla gestione del cambiamento e alla definizione di un modello di governance per l'attuazione dei progetti e per il raggiungimento degli obiettivi.

Il coinvolgimento dell'ICT è ovvio e riguarda una pluralità di soggetti diversi fra loro, sia nella funzione che nell'organizzazione, è auspicabile pertanto una crescita sistemica della governance attraverso strumenti digitali sensibili al contesto, nel rispetto dei tempi e linee di azione stabilite dal Governo e dall'Università di Firenze.

L'eterogeneità dei progetti inseriti nel Piano Integrato dell'Università di Firenze prevede la partecipazione attiva dell'Area dell'Innovazione e Gestione dei Servizi Informativi ed Informatici per il raggiungimento di obiettivi specifici con peculiarità tecnologiche e metodologiche, in particolare negli ambiti del miglioramento dei servizi per gli studenti, della comunicazione e public engagement, della valorizzazione del patrimonio e gestione delle risorse umane.

Saranno messe a disposizione le competenze organizzative, digitali, tecnologiche ed innovative a supporto di quelle didattiche, amministrative e della terza missione sia per la realizzazione dei progetti sia per far crescere le strutture in termini di competenze digitali avanzate, aggregare la domanda di innovazione ed ottimizzare la comunicazione ed i servizi dal punto di vista digitale. Si adotteranno a tale scopo ecosistemi digitali, metodologie di condivisione della conoscenza e monitoraggio, attraverso specifiche tecniche di project management e knowledge management.

AgID raccomanda alle PA di applicare i principi ritenuti fondamentali per la realizzazione dei progetti contenuti nel Piano triennale per l'informatica nella pubblica amministrazione 2017-2019. Gli accorgimenti riguardano la gestione del progetto e le regole contrattuali e amministrative per la stesura del contratto, la definizione degli obiettivi, e l'approvvigionamento delle risorse (Cloud Marketplace di AgID).

La metodologia per i progetti digitali suggerita è agile, per la realizzazione di nuovi sistemi o per l'evoluzione di sistemi esistente richiede:

- un chiaro disegno di cosa si vuole ottenere (design);
- un piano di come costruirlo (realizzazione);
- una strategia per portarlo all'adozione degli utenti finali (lancio);
- un piano per mantenere il sistema aggiornato, sicuro, e utile nel tempo, oltre che per assicurarne il continuo funzionamento anche in caso di malfunzionamenti o disastri (evoluzione e manutenzione).

Oltre alle linee guida di AgID, il gruppo di Enterprise Architecture e Project Management Office (EAPMO), nel perseguire le finalità della mission dell'Area per l'Innovazione e Gestione del Sistemi Informativi ed Informatici, costituisce un supporto delle attività di pianificazione e monitoraggio nell'ambito della funzione trasversale dell'innovazione per lo sviluppo sinergico dei processi di informatizzazione dell'Ateneo.

In questa ottica nel 2018 è stato intrapreso un percorso di analisi oltre che formativo per l'individuazione delle metodologie e strumenti di project management da utilizzare. Il suddetto percorso ha riguardato la gestione dei "progetti pilota" di SIAF con prospettive di tipo metodologico ed operativo in base ai compiti specifici del PMO.

Gli obiettivi a breve e medio termine dal punto di vista metodologico, che si ritengono fondamentali e che costituiranno l'asset del PMO dell'Area, riguardano principalmente la definizione di: set di strumenti organizzativi, regole operative, modalità di reporting, assistenza metodologica e operativa, dati e documenti di progetto, modalità di archiviazione (in cloud, codifica documentale, censimento dei servizi), coaching su tecniche di project management e comportamentali, sistemi di comunicazione, projects reviews, projects integration, projects portfolio, divulgazione di best practices.

Operativamente le attività di governance dei progetti sono rivolte a decidere la metodologia da applicare (tradizionale, kanban, scrum), creare template e check list operative, delineare ruoli e responsabilità, definire i team di progetto (competenze funzionali e manageriali), individuare i progetti pilota, definire una roadmap per l'applicazione delle metodologie, rilevare le metriche di misurazione e obiettivi.

È prevista l'adozione di una piattaforma in cloud al fine di governare la pianificazione e il monitoraggio dei progetti nonché per la gestione della conoscenza (knowledge management), decisione scaturita dopo una prima analisi di scenari e piattaforme individuate nel corso del 2018.

2 Sicurezza informatica

La transizione al digitale della pubblica amministrazione richiede che si ponga sempre maggiore attenzione alla sicurezza informatica che non può semplicemente ridursi alla mera applicazione di misure tecniche di contrasto passivo, ma che deve permeare l'organizzazione in maniera profonda partendo dai processi (e quindi dal livello organizzativo) e dai principi di base ispiratori di una politica di sicurezza diffusa e consapevole.

Ai temi richiamati dal GDPR quali "privacy by default" si affianca quindi oggi una necessità più ampia che potremmo definire come "digital by default" che andrà ad impattare pesantemente sulle infrastrutture IT di aziende e pubbliche amministrazioni.

Si stima che al 2020 gli utenti Internet passeranno da 3.5 miliardi a 6 miliardi e che il volume di dati online crescerà di circa 50 volte passando da 4 zettabyte (4000 miliardi di miliardi di byte) a quasi 100 zettabyte con le conseguenze che possiamo facilmente immaginare sui rischi potenziali di accesso e diffusione di dati personali e strategici.

Le conclusioni dei principali analisti in tema di sicurezza informatica circa l'analisi degli incidenti informatici e delle minacce diffuse negli ultimi anni sono allarmanti sia per i danni economici diretti, sia perché almeno in Italia circa il 60% degli intervistati ammette di non avere un piano di risposta ad eventuali attacchi informatici sia dal punto di vista tecnico che dal punto di vista della comunicazione; la situazione a livello mondiale non è certamente migliore come ad esempio il famoso caso di Equifax che ha esposto i dati oltre 140 milioni di cittadini americani evidenziando come l'assenza di un piano di risposta agli incidenti testato e definito possa impattare negativamente sugli effetti di un incidente informatico.

Tenendo presente questi fattori è necessario quindi che la sicurezza informatica diventi al pari delle tematiche in termini di privacy una priorità centrale per il nostro Ateneo con investimenti in termini di risorse umane destinati a crescere nel tempo.

La strategia di breve termine deve focalizzarsi sulla possibilità di identificare una serie di misure operative atte a ridurre il rischio e soprattutto finalizzate ad aumentare la consapevolezza del rischio stesso in ambito digitale: è fondamentale infatti far percepire che la sicurezza informatica non è più ormai una realtà che coinvolge solo le aziende (siano esse private o pubbliche amministrazioni) ma che permea la vita di ogni cittadino. Operare quindi secondo maggiori canoni di sicurezza non è solo utile quando si lavora, ma anche nella vita quotidiana e quindi l'impatto positivo di una maggiore consapevolezza si espande ben oltre i confini dell'azienda.

Se fornire quindi delle istruzioni operative congrue ai tempi è una operazione da compiere nel brevissimo termine, non ci possiamo scordare di azioni da intraprendere nel medio periodo che devono indirizzare il processo di gestione della sicurezza informatica a livello più strategico e con una gestione orientata al miglioramento continuo.

Sempre nel breve termine è necessario focalizzare l'attenzione sulla revisione delle politiche di gestione degli incidenti includendo anche le segnalazioni minori ed i potenziali incidenti in modo da avere un monitoraggio più puntuale delle attività effettuate e del rischio presente; identificare un maggior numero di incidenti non è sintomo di peggiore gestione della sicurezza informatica ma di maggiore consapevolezza dei rischi potenziali nell'ottica delle strategie di mitigazione e gestione degli incidenti stessi. Monitorare quindi delle metriche quantitative relative agli incidenti potrebbe essere utile per capire come stiano variando le condizioni al contorno ed in questa logica la realizzazione di una piattaforma per la storicizzazione degli incidenti è un punto centrale per migliorarne la gestione.

Una delle azioni fondamentali di medio termine invece sarà quella di creare una "Information Security Policy" che oltre a contenere i principi ispiratori generali per l'adozione di una opportuno livello di sicurezza informatica, definisca delle politiche per ogni area ritenuta strategica identificando le misure organizzative e le indicazioni relative alle misure tecniche da implementare; questo documento è di tipo organizzativo e di indirizzo più che una lista di misure tecniche da adottare e per questo è necessaria la massima condivisione a livello politico. Le misure identificate come strategiche dovranno quindi essere divise fra quelle già in essere, quelle da realizzare nel breve termine e quelle da implementare nel medio termine monitorando con metriche quantitative il processo di adozione.

Solo a valle di questa impostazione di alto livello sarà possibile declinare le misure tecniche necessarie affinché quelle di indirizzo siano correttamente rispettate ed implementate realizzando quindi un documento contenente una proposizione di architettura di sicurezza in cui siano più puntualmente indirizzate anche le indicazioni AgID contenute nella Circolare relativa alle misure minime.

Questo processo di redazione dovrà, secondo il principio del miglioramento continuo, essere soggetto a revisioni periodiche con verifiche degli stati di avanzamento per valutare come migliorare la sicurezza informatica sia a livello tecnico che organizzativo.

8 Ecosistemi e infrastrutture fisiche

La strategia di razionalizzazione delle risorse ICT della PA anche nell'ottica dei PSN (Poli Strategici Nazionali) costringe ad una riflessione profonda sulle tecnologie da utilizzare all'interno dei Data Center correnti dell'Ateneo sia per scopi di ricerca che per la gestione dell'infrastruttura di supporto ai servizi erogati all'interno ed all'utenza. A questa riflessione si aggiungono le considerazioni sul numero sempre più ridotto di persone dedicate al mantenimento dell'infrastruttura ICT che ci spinge verso logiche di outsourcing e/ consolidamento verso tecnologie standard di mercato per le quali si possano reperire competenze certificate in tutte le situazioni in cui non sia possibile operare con le sole risorse interne o per situazioni di emergenza.
A queste riflessioni si aggiungono poi i temi dello spostamento verso il Cloud di alcune risorse sia per garantire la continuità operativa che per permettere un più efficace utilizzo delle risorse economiche in termini di utilizzo e pagamento on demand dei servizi necessari.
Sicuramente la scelta tecnologica non è indifferente in termini di effetti in questo contesto, in quanto è necessario andare nella logica del consolidamento delle tecnologie riducendo la diversificazione tecnologica, ove possibile, per riuscire ad ottimizzare sia i processi di formazione continua che l'interscambiabilità delle risorse nella gestione ICT. Nella scelta della tecnologia, oltre alle necessità computazionali e di espansione dell'Ateneo, sono state prese in considerazione molti fattori tra quali:

- La convenienza di tipo economico sfruttando le convenzioni esistenti alle quali fosse possibile accedere
- La valutazione della tecnologia sul mercato e la sua diffusione in modo da facilitare una futura integrazione o spostamento verso i PSN o il CloudPA nel momento in cui se ne dovesse manifestare la necessità
- La possibilità di condividere con altri Atenei la scelta tecnologica al fine di trovare sinergie
- La maturità tecnologia delle soluzioni per affrontare temi diversi quali la virtualizzazione di server eterogenei e la fruizione di desktop virtuali da poter utilizzare sia per scopi didattici (aule, supporto alle biblioteche) che per utilizzi in ambito tecnico/amministrativo (telelavoro, personale T/A, etc)
- La tipologia di applicativi che si devono gestire

Università di Firenze ha attivato dal 2018 una convenzione con la Regione Toscana nell'ottica di condividere il Data Center regionale TIX e collaborare per la sua certificazione come PSN (Polo Strategico Nazionale) in linea con le strategie del Piano Triennale.
Tutte queste considerazioni hanno spinto l'Ateneo verso l'adozione della soluzione iperconvergente VMWare che oltre a coprire le necessità offre la necessaria versatilità in termini di espandibilità futura.
Si intendono attivare nel breve termine due cluster, uno identificato come General Purpose dedicato ad ospitare diversi server sia dedicati agli applicativi dell'amministrazione centrale che a progetti di ricerca o di didattica e un'altro dedicato a sup-

portare i Thin Client delle aule informatiche, delle aule didattiche e delle postazioni al pubblico e per fornire un servizio più sicuro per il telelavoro.

Su questa nuova piattaforma saranno migrati sia i server attualmente nel cluster presso Novoli che i vdi sul cluster attualmente in produzione e come ulteriore fase di consolidamento possiamo considerare la migrazione di parte dei server fisici o virtuali ospitati al momento in Rettorato. Inoltre, sarà possibile consolidare diversi server fisici ancora presenti in alcune strutture di Ateneo.

A tendere, anche le piattaforme Moodle ed altri servizi potranno convergere su questa nuova architettura consolidando su una interfaccia unica ed uniforme più servizi possibili in ottica di aggiornamento continuo alle tecnologie di mercato.

A livello di integrazione con la gestione della sicurezza informatica, questa nuova piattaforma ospiterà anche un sistema Active Directory sulla quale sarà possibile centralizzare la gestione anche delle aule con PC fisici nonché la gestione delle postazioni del personale tecnico amministrativo permettendone una più agevole gestione e manutenzione centralizzando alcune operazioni ad oggi possibili solo operando singolarmente su ogni PC.

Al fine di garantire il backup dell'infrastruttura è stato previsto un doppio target di backup, in cui il target secondario sia ospitato nel breve termine presso il TIX avendo quindi la possibilità di avere una copia dei dati e dei server fuori sede al fine di garantire un disaster & recovery con dati delocalizzati, ma fruibili indipendentemente dall'hardware necessario a recuperarli; nel medio termine non si esclude anche la possibilità di avere un ulteriore livello di salvataggio su nastro da portare in una sede diversa. In caso di disastro del sito principale di SIAF infatti l'esportazione dei dati su nastro e la conservazione in una sede diversa garantisce sicuramente la conservazione del dato, ma se la libreria per la rilettura dei nastri non fosse disponibile difficilmente potremmo far ripartire i servizi o recuperare i dati i tempi brevi, mentre la disponibilità di dati online in una sede diversa permetterebbe in linea teorica una ripartenza dei servizi prendendo ad esempio dei servizi di hosting in cloud tramite i servizi offerti da CloudPA, dal TIX stesso o da provider reputati opportuni.

Questo tipo di attività potrebbe essere il primo passo per mettere in piedi un vero e proprio piano di continuità operativa delle infrastrutture tecnologiche fondamentali per il funzionamento dell'Ateneo.

Oltre alla parte strettamente di infrastruttura di DataCenter è in corso il potenziamento anche dell'infrastruttura WiFi. L'Ateneo ha infatti avviato un progetto per estendere la copertura del segnale wireless per l'accesso alla rete universitaria ed Internet in tutte le aule didattiche e informatiche presenti negli edifici dell'Ateneo.

Il progetto rientra in un contesto più ampio che prevede ristrutturazione, ampliamento e messa in sicurezza di aule e laboratori. Questo processo ha preso inizio con l'acquisizione di una seconda tecnologia da affiancare all'attuale tecnologia Cisco, per estendere l'infrastruttura wireless nelle aule di Ateneo in maniera integrata, efficiente e performante. Per l'individuazione della seconda tecnologia, per motivi amministrativi, si è reso necessario valutare dal punto di vista tecnico l'offerta presente in Convenzione Consip denominata LAN 6 Reti Locali, basata su tecnologia Huawei. Nella valutazione tecnologica sono stati considerati aspetti funzionali mirati a fornire connettività in ambienti ad alta densità di client, come di seguito descritto:

- connessione ad una rete wifi con autenticazione secondo modalità diverse e funzionali alle esigenze attuali e future dell'Ateneo;
- possibilità di definire una banda minima garantita per dispositivo;
- distribuzione evoluta dei dispositivi tra gli access point attivi;
- Connessione simultanea con le specifiche precedenti di 500 dispositivi in ambienti ristretti.

In questo ambito, SIAF si pone l'obiettivo di fornire servizi di connettività wireless all'interno di locali o, più genericamente, spazi ristretti densamente frequentati da 250-300 studenti, personale docente e tecnico amministrativo, valutando una densità massima di client wifi che potrà raggiungere e superare le 500 unità. È verosimile, infatti, considerare la dotazione di due dispositivi wifi a persona, generalmente costituiti da uno smartphone ed un computer portatile o tablet. Altro obiettivo dell'infrastruttura WIFI è di mantenere un'architettura centralizzata basata su controller per una gestione semplificata ed un monitoraggio efficace dell'intera infrastruttura.